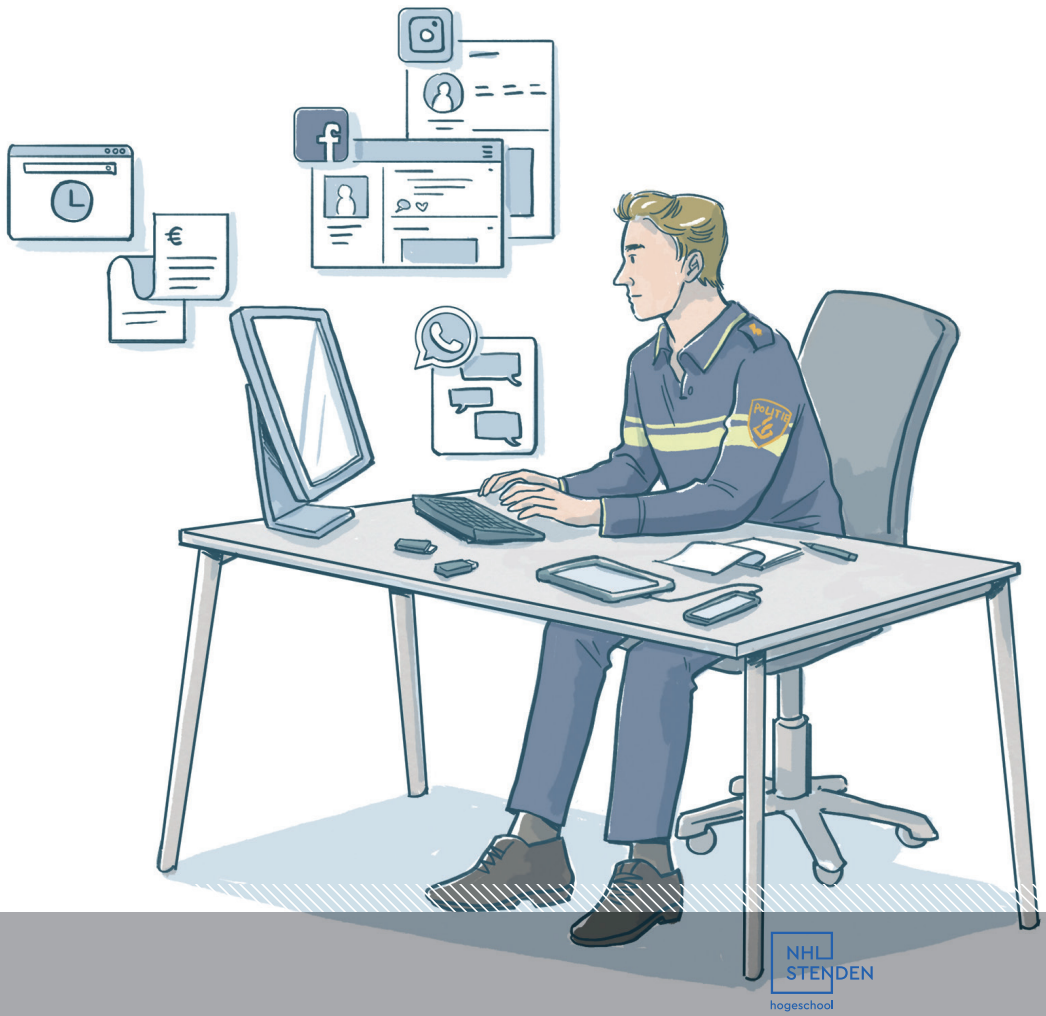
POLITIE & Wetenschap

Benutten van digitale sporen

R. Zuurveen, W.Ph. Stol



NHL STENDEN hogeschool

Benutten van digitale sporen

Benutten van digitale sporen

R. Zuurveen
W.Ph. Stol

POLITIE & Wetenschap

NHL STENDEN hogeschool

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:
Sdu Klantenservice
Postbus 20025
2500 EA Den Haag
tel.: (070) 378 98 80
website: www.sdu.nl

Omslagontwerp: Imago Mediabuilders, Amersfoort
Afbeelding omslag: Yuran Choi (studioyknot.myportfolio.com)

ISBN: 9789012406420
NUR: 600

Inhoudsopgave

Ten geleide

Dit onderzoek is uitgevoerd door de Onderzoeksgroep Cybersafety van NHL Stenden Hogeschool en Politieacademie in opdracht van Politie & Wetenschap

Renske Marskamp-Zuurveen MSc LLM
Prof. dr. Wouter Stol

Met medewerking van:
dr. Willem Bantema
dr. Jurjen Jansen
Elske Posthuma LLM
Mirjam Uenk MSc
Jan Aink MSc

Met dank aan het consortium:
Alwin Hilberink
Richard Nijeboer
Christianne de Poot
Anton van Wijk

Begrippen en afkortingen

Deze lijst bevat afkortingen en enkele specifieke begrippen. Afkortingen en begrippen die slechts op één plaats in de tekst voorkomen, zijn niet hier maar op die plaats toegelicht.

BOB	Bijzondere Opsporingsbevoegdheden
Cybercrime Team	Iedere regionale eenheid binnen de politie heeft een Cybercrime Team. Dit team bestaat uit politiemensen die zich primair bezighouden met de bestrijding van cybercrime.
DCS	Digitale Communicatie Sporen (softwareprogramma om historische telefoongegevens te analyseren)
DRIO	Dienst Regionale Informatie Organisatie
DRR	Dienst Regionale Recherche
EXIF	Exchangeable Image File Format. Bevat metadata over een fotobestand, bijvoorbeeld datum en tijd waarop de foto is gemaakt, merk/model camera, gps-gegevens, camera-instellingen, etc.
iRN	internet Research and Investigation Network. Met iRN kan de politie op relatief anonieme en veilige wijze onderzoek verrichten op internet.
IP-adres	Internet Protocol-adres
LMIO	Landelijk Meldpunt Internet Oplichting
MAC-adres	Media Access Control-adres. Vrij uniek nummer dat is gekoppeld aan ieder hardwarecomponent met een netwerkfunctionaliteit. Zo heeft een smartphone een WiFi-MAC-adres en een Bluetooth-MAC-adres. Het kan worden gebruikt om bijvoorbeeld een computer te identificeren binnen een intern netwerk.
Metadata	Secundaire informatie dat wordt opgeslagen samen met een digitaal bestand (data over data). Uit metadata van een document kunnen bijvoorbeeld auteur, datum van schrijven en het aantal pagina's worden achterhaald.
Modem	Een modem verzorgt de koppeling tussen het netwerk van de provider en het interne (thuis)netwerk. Meestal is de functionaliteit in een apparaat geïntegreerd met de router en het WiFi-access point.
Nickname	Bijnaam

OSINT	Open Source Intelligence
Pd	Plaats delict
P.v.	Proces-verbaal
Router	Apparaat dat de goede aflevering van internetverkeer tussen twee netwerken verzorgt (zoals het netwerk van de provider en het interne netwerk).
Summ-IT	Summ-IT is een politieregistratiesysteem van de Nederlandse politie en de opvolger van de Basis Voorziening Opsporing (BVO).
Tapper	Deskundige op het gebied van het aftappen van berichtenverkeer.
TBKK	Team Bestrijding Kinderporno en Kindersekstoerisme
TCI	Team Criminele Inlichtingen
TDO	Team Digitale Opsporing
THTC	Team High Tech Crime
UCO	Uitlezen Communicatiemiddelen. Onderwijsmodule van de Politieacademie.
UFED	Universal Forensic Extraction Device. Tool waarmee onderzoek wordt verricht aan mobiele telefoons.

1. Inleiding

1.1 Aanleiding tot dit onderzoek

"Digitaal bewijs wordt misschien wel belangrijker dan DNA-bewijs", zei Hans Henseler, lector forensisch ICT aan de hogeschool van Leiden, in EenVandaag[1] naar aanleiding van de recente vermissingszaak van Anne Faber. Met de telefoongegevens van Anne kon haar fietsroute in kaart worden gebracht en haar exacte locatie toen ze een selfie maakte. Dat waren twee belangrijke aanknopingspunten voor het onderzoek.

In de huidige tijd laten mensen steeds vaker digitale sporen achter. Een zoekmachine raadplegen, een e-mail versturen, maar ook een foto maken, autorijden en simpelweg op straat lopen: al deze activiteiten creëren digitale gegevens en dus bewijsmateriaal (Daniel & Daniel, 2012). Deze trend zorgt ervoor dat politiemensen bij het beoefenen van hun vak steeds vaker te maken kunnen krijgen met digitale sporen. Inmiddels kent vrijwel ieder delict, ook een klassiek offline delict, een digitale component (ACPO, 2011; Domenie, Leukfeldt, Van Wilsem & Stol, 2012; MacNeil, 2015; Stol & Jansen, 2013).

Het gebruik van digitale sporen is in dit onderzoek gedefinieerd als het gebruik van alle data die is opgeslagen op of verzonden met een device, zoals een smartphone of laptop (Casey, 2011). Deze definitie is ook als zodanig genoemd bij geïnterviewden en respondenten waarbij voorbeelden werden genoemd als: internetgeschiedenis, social media, Whatsapp-berichten, bankgegevens, geotags[2] en e-mailheaders[3]. Sporen die in dit onderzoek niet vallen onder digitale sporen zijn camerabeelden en foto's. We hebben ons daarmee gericht op digitale sporen die de afgelopen vijf jaar steeds meer op de voorgrond treden en steeds belangrijker zijn geworden in ieders dagelijks leven – en daarmee ook in vrijwel ieder opsporingsonderzoek.

De politie profiteert te weinig van de mogelijkheden die digitale sporen bieden voor de opsporing (Junger, Montoya, Hartel & Karemaker, 2013; Rompu, 2015; Stol, Leukfeldt & Klap, 2013). Veenstra, Zuurveen, Kerstens en Stol (2016) concluderen uit onderzoek

1 Uitzending van 7 oktober 2017.
2 Een geotag bevat informatie over de geografische locatie van bijvoorbeeld een foto.
3 Een e-mailheader bevat informatie over onder meer de afzender van het bericht.

onder digitaal experts, rechercheurs en medewerkers uit de basisteams dat in vrijwel alle zaken digitale sporen een bijdrage kunnen leveren, maar dat daarvan in de praktijk weinig gebruik wordt gemaakt.

Al in 2004 zei Wouter Stol, lector Cybersafety, dat een gebrek aan kennis over de digitale wereld een primaire hindernis is voor de politie (Stol, 2004). Nicolien Kop, lector Criminaliteitsbeheersing en Recherchekunde, spreekt van een "digitale generatiekloof" als gevolg van "jarenlang achterstallig onderhoud" (Haenen, 2015). Bij politiemedewerkers zonder digitale expertise is er onvoldoende kennis over het uitlezen van gegevensdragers en de internettap, waardoor digitale sporen onzichtbaar blijven (Odinot, Jong & Van der Leij, 2012; Veenstra e.a., 2016). Hoewel de politie prioriteit geeft aan cybercrime en er steeds meer digitaal specialisten in dienst zijn, is kennis van digitalisering nodig in de volle breedte van de politieorganisatie (Stol e.a., 2013). De laatste jaren zijn stappen gezet in de goede richting, maar het kennistekort is nog niet opgelost. Zo concludeert Van Valkengoed in een onderzoek bij de politie in Amsterdam naar kennis omtrent opsporing van cybercrime, dat rechercheurs op verschillende niveaus (regio, district, basisteam) "niet voldoen aan de vereisten van basiskennis" en "niet voldoen aan de vereisten van basisvaardigheid". Wel bezitten rechercheurs volgens dit onderzoek "de noodzakelijke attitude" (Van Valkengoed, 2017, p. 52-53).

Kortom, vandaag de dag zijn bij vrijwel ieder delict digitale sporen te verwachten. Het lijkt er echter op dat de politie van digitale sporen veelal (veel) te weinig gebruikmaakt. Zo gezien lijkt voor de politie daar dus winst te halen.

De aanleiding tot dit onderzoek is de vraag of 'kennistekort' wel een voldoende verklaring is voor het gesignaleerde achterblijven van het gebruik van digitaal bewijs. Dit onderzoek heeft dan ook tot doel om vast te stellen wat de achterliggende motieven en overwegingen van politiemensen zijn voor het al dan niet gebruiken van digitale sporen. Aan de hand van die inzichten kunnen mogelijk gerichte interventies ingezet worden om het gebruik van digitale sporen te bevorderen, ten gunste van de opsporing.

1.2 Leeswijzer

Na een bespreking van het onderzoek en de onderzoeksmethoden in hoofdstuk 2 en 3 wordt in hoofdstuk 4 ingegaan op de mogelijkheden en knelpunten bij het benutten van digitale sporen. Dit hoofdstuk is geschreven op basis van literatuuronderzoek en interviews. Hoofdstuk 5 gaat over het gebruik van digitale dan wel analoge sporen in het casusonderzoek en over het gebruik van digitale sporen in het algemeen. In hoofdstuk 6 worden de intenties voor het gebruik van digitale sporen besproken en de relatie met daadwerkelijk gebruik van digitale sporen. De conclusies staan centraal in hoofdstuk 7. We sluiten af in hoofdstuk 8 met het bespreken van de beperkingen van het onderzoek.

In dit rapport wordt gebruik gemaakt van specifieke vaktermen. Voor het overzicht – en om herhaling te voorkomen – is voorin dit rapport een begrippen- en afkortingenlijst opgenomen.

2. Doel- en vraagstelling

2.1 Doelstelling

Het doel van dit onderzoek is het bieden van inzicht in motieven en overwegingen van politiemensen voor het al dan niet gebruiken van digitale sporen en het vertalen van de bevindingen naar verbetering van de opsporingspraktijk. Het hoger gelegen doel is een bijdrage te leveren aan de effectiviteit van de opsporing.

2.2 Vraagstelling

De aanleiding tot dit onderzoek is de vraag of kennistekort wel een voldoende verklaring is voor het gesignaleerde geringe gebruik van digitale sporen. Dit onderzoek wil inzicht verwerven in de achterliggende motieven en overwegingen voor het al dan niet gebruiken ervan. Daaruit volgt als hoofdvraag van dit onderzoek: 'Welke motieven en overwegingen hebben politiemensen voor het al dan niet gebruiken van digitale sporen en hoe kunnen deze bevindingen worden vertaald naar het verbeteren van de opsporingspraktijk?' De hoofdvraag is opgesplitst in deelvragen:

1. Welke niet-technische factoren belemmeren het tactisch gebruik van digitale sporen door politiemensen (zoals praktische, juridische en mentale factoren)?

2. In hoeverre en op welke wijze gebruiken politiemensen digitale sporen bij opsporingsonderzoek?
    1. Aan welke zoekstrategie – digitaal of analoog – geven politiemensen de voorkeur wanneer ze opsporingsonderzoek verrichten, en waarom?
    2. Hoe gebruiken politiemensen digitale sporen bij opsporingsonderzoek?

3. In hoeverre hebben politiemensen de intentie om digitale sporen te gebruiken bij opsporingsonderzoek en in hoeverre handelen ze naar hun intenties?
    1. In hoeverre hebben politiemensen de intentie om digitale sporen te gebruiken?
    2. In hoeverre handelen politiemensen naar hun intenties om digitale sporen te gebruiken?
    3. Door welke factoren kan een eventuele discrepantie tussen de intentie om digitale sporen te gebruiken en het daadwerkelijke gebruik ervan worden verklaard?

3. Onderzoeksmethoden

3.1 Overzicht: methodenmatrix

Er zijn meerdere onderzoeksmethoden gebruikt om de onderzoeksvragen te beantwoorden (triangulatie): literatuuronderzoek, juridisch bronnenonderzoek, interviews en een casusonderzoek. Tabel 3.1 toont de methoden per deelvraag. De methoden worden hierna achtereenvolgens besproken.

Tabel 3.1: Methodenmatrix

	Literatuur-onderzoek	Interviews	Casus-onderzoek	Vragenlijst
1.Belemmerende factoren	x	x		
2.Gebruik van digitale sporen?		x	x	x
3.Handelen naar intenties?			x	x

3.2 Literatuuronderzoek

Literatuuronderzoek is ingezet om deelvraag 1 te beantwoorden, te weten: welke niet-technische factoren belemmeren het tactisch gebruik van digitale sporen door politiemensen (zoals praktische, juridische en mentale factoren)? Hiertoe zijn wetenschappelijke databases geraadpleegd, zoals ScienceDirect en Web of Science, en juridische databases als Rechtsorde en www.rechtspraak.nl. Zoektermen die, al dan niet in combinatie met elkaar, zijn gebruikt waren bijvoorbeeld: 'digitaal bewijsmateriaal', 'digitale sporen' en 'knelpunt praktisch'. Daarbij werden ook verwante zoektermen gebruikt als 'digitaal bewijsmateriaal' en 'belemmering juridisch'. Omdat zowel nationale als internationale literatuur is geraadpleegd, werd ook gezocht op Engelstalige zoektermen als 'digital evidence' en 'digital traces'.

3.3 Interviews

Interviews zijn afgenomen met zowel experts als politiemensen in het opsporingsproces. Er zijn tussen 5 december 2018 en 14 januari 2019 zeven semigestructureerde interviews afgenomen met experts binnen en buiten de justitiële keten. Tabel 3.2 bevat een overzicht van de geïnterviewde experts en hun functies.

Tabel 3.2: Geïnterviewde experts

Naam	Functie(s)
Arnout de Vries	Onderzoeker en adviseur op het gebied van internet en maatschappelijke veiligheid bij TNO
Erik Gritter	Universitair docent Straf(proces)recht, met expertise IT-recht
Ruud Elderhorst	Strategisch digitaal specialist bij Team Digitale Opsporing, Eenheid Den Haag
Martijn Egberts	Landelijke officier van justitie cybercrime
Edwin Posthumus*	Strategisch digitaal specialist bij Team Digitale Opsporing, Eenheid Noord-Nederland
Harry Lassche	Docent Politieacademie, expertise op het gebied van digitalisering en de opsporingspraktijk
Marjolein Viersma	Adviseur digitale opsporing/juridisch expert, Dienst Regionale Recherche, Eenheid Amsterdam

*Bij het gesprek sloten twee collega's aan van Team Digitale Opsporing Noord-Nederland.

Ter aanvulling op de expertinterviews zijn drie interviews afgenomen met in totaal zes rechercheurs zonder digitale expertise. Eén interview betrof een groepsinterview met vier rechercheurs. Dit interview vond plaats op 19 december 2018. De overige twee interviews waren één-op-één met twee rechercheurs op 16 en 17 januari 2019. Alle rechercheurs waren werkzaam bij de Eenheid Noord-Nederland. Dit laatste is mogelijk van invloed op de generaliseerbaarheid van de resultaten. Hierop gaan we in hoofdstuk 8 dieper in. De interviews zijn gebruikt om deelvraag 1 te beantwoorden. Voorafgaand aan de interviews is een interviewprotocol opgesteld. Dit protocol is opgenomen in bijlage 1.

In totaal zijn dus dertien personen geïnterviewd. Alle interviews zijn face-to-face afgenomen. De interviews zijn – met toestemming van de geïnterviewden – opgenomen met een opnameapparaat voor uitwerkingsdoeleinden. De interviewdata zijn geanalyseerd door twee onderzoekers met behulp van Atlas.ti. Alle informatie uit de interviews is teruggebracht tot specifieke factoren en overkoepelende thema's. Vervolgens zijn alle uitspraken van de verschillende respondenten geclusterd per factor. Relevante citaten uit de interviews zijn verwerkt ten behoeve van het beantwoorden van deelvraag 1.

3.4 Casusonderzoek

Het casusonderzoek vormde de input om de deelvragen 2 en 3 te beantwoorden: 2) in hoeverre en op welke wijze gebruiken politiemensen digitale sporen bij opsporingsonderzoek, en 3) in hoeverre hebben politiemensen de intentie om digitale sporen te gebruiken bij opsporingsonderzoek en in hoeverre handelen ze naar hun intenties?

Casus
Bij aanvang van het experiment kregen respondenten een casus te lezen. De casus is opgenomen in bijlage 2. Vervolgens kregen de respondenten om de casus op te lossen de instructie om steeds een keuze te maken tussen twee bewijsstukken (digitaal of analoog, dus niet beide), gebaseerd op hun voorkeur. Ook werd aangegeven dat, hoewel normaal gesproken mogelijk voor beide bewijsstukken zou worden gekozen, voor dit onderzoek slechts één van de twee gekozen kon worden.

De casus is geïnspireerd op een bestaande zaak die speelde bij de politie in Drenthe. In samenwerking met twee politiemensen is de casus verder geoptimaliseerd en zijn de tien keuzes behorend bij de casus opgesteld. Tijdens het casusonderzoek zijn er door de respondenten geen opmerkingen gemaakt over het realistische gehalte van de casus dan wel de bijbehorende keuzes. We gaan er daarom in beginsel vanuit dat de casus passend was voor de huidige politiepraktijk.

Er diende steeds een keuze te worden gemaakt tussen twee bewijsstukken: een digitaal en een analoog bewijsstuk. De waarde van het bewijsstuk – de bijdrage die het levert aan het achterhalen van de verdachte en bewijs van daderschap – was bij beide soorten bewijsstukken hetzelfde. Ook het resultaat (positief dan wel negatief) was bij beide hetzelfde. De digitale variant van een bewijsstuk was bijvoorbeeld een analyse van de contacten op Instagram en Facebook van aangeefster en de analoge variant van het bewijsstuk betrof de resultaten van een buurtonderzoek in de omgeving van de pd. Beide bewijsstukken leverden op dat de verdachte vriendschappelijke contacten onderhield met een getuige/katvanger. In totaal zijn tien keuzes voorgelegd. Bij vijf keuzes was het resultaat van beide bewijsstukken positief en bij vijf negatief.

Keuzeverantwoording en nagesprek
Direct na het maken van iedere keuze werden drie vragen voorgelegd:
– Waarom heb je voor dit bewijsstuk gekozen?
– Waarom heb je het andere bewijsstuk NIET gekozen?
– Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan?

Daarnaast is aan het einde van de casus gevraagd of respondenten verder nog iets wilden zeggen over hun ervaringen met het gebruik van digitale sporen. Om verder inzicht te krijgen in de invloed van een positief dan wel negatief resultaat van een bewijsstuk[4] is na afloop gevraagd of het resultaat van ieder bewijsstuk invloed heeft gehad op de daaropvolgende keuze. Tot slot is gevraagd om een algemene toelichting te geven op de gemaakte keuzes.

4 Zie bijlage 2: vijf bewijsstukken hebben, ongeacht of het een analoge of digitale keuze betreft, een negatief resultaat en vijf bewijsstukken hebben een positief resultaat.

Werving van respondenten
De respondenten zijn ten eerste geworven in samenwerking met twee teamchefs. Zij hebben een oproep voor het onderzoek geplaatst op intranet en hebben de uitnodiging voor het onderzoek per e-mail gedeeld met hun team. Ten tweede zijn respondenten geworven door het netwerk van de onderzoekers in te zetten. Hoewel de instructie is gegeven om woorden als 'digitale sporen' en 'cybersafety' niet te noemen in de oproep op intranet, is dat bij de Eenheid Noord-Nederland toch gebeurd. Daardoor kan het zijn dat respondenten hebben deelgenomen die meer dan de gemiddelde politiemedewerker interesse hebben in het thema. Daar gaan we in hoofdstuk 8 dieper op in. In bijlage 4 staat een gedetailleerde uiteenzetting van de werving van respondenten.

Uiteindelijk hebben 76 respondenten deelgenomen aan het casusonderzoek: drie uit Eenheid Noord-Holland, zeventien uit de Eenheden Oost- en Midden-Nederland en 56 uit Eenheid Noord-Nederland. Het casusonderzoek vond plaats tussen 4 april 2019 en 17 mei 2019.

Beschrijving van respondenten
Deze sectie beschrijft de respondenten in meer detail. Een volledig overzicht staat in bijlage 5. Het geboortejaar 1976 is de mediaan van de steekproef (42/43 jaar). De oudste deelnemer had als geboortejaar 1955 en de jongste 1993. Er hebben 49 mannen deelgenomen (64,5%) en 27 vrouwen (35,5%). De meeste respondenten (N=51) zijn langer dan tien jaar werkzaam voor de politie. Elf respondenten hebben een dienstverband tussen de vijf en tien jaar. In mindere mate zijn respondenten drie tot vijf jaar (N=9) en één tot drie jaar (N=5) werkzaam bij de politie.

De drie meest genoemde functies die de respondenten vervullen binnen de politie zijn: generalist (N=28), operationeel specialist (N=16) en senior (N=14). Operationeel experts (N=9), aspirant recherchekundigen (N=6) en medewerkers/assistenten (N=3) namen in mindere mate deel aan het casusonderzoek. Ook is gevraagd naar de precieze werkzaamheden die respondenten vervullen binnen de politie. De volgende werkzaamheden werden vaker dan één keer genoemd:[5] tactisch rechercheur bij de districtsrecherche (N=20), politiemedewerker in uniformdienst (N=14), tactisch rechercheur bij de basisteamrecherche (N=12), tactisch rechercheur bij de regionale recherche (N=11), aspirant recherchekundige (N=6), medewerker intelligence (N=3) en zedenrechercheur (N=2).

Om inzicht te krijgen in de ervaring met digitale sporen is gevraagd in hoeverre respondenten hiertoe een opleiding/cursus hebben gevolgd en de mate waarin ze er tijdens hun werkzaamheden mee te maken hebben gehad. 35 respondenten gaven aan

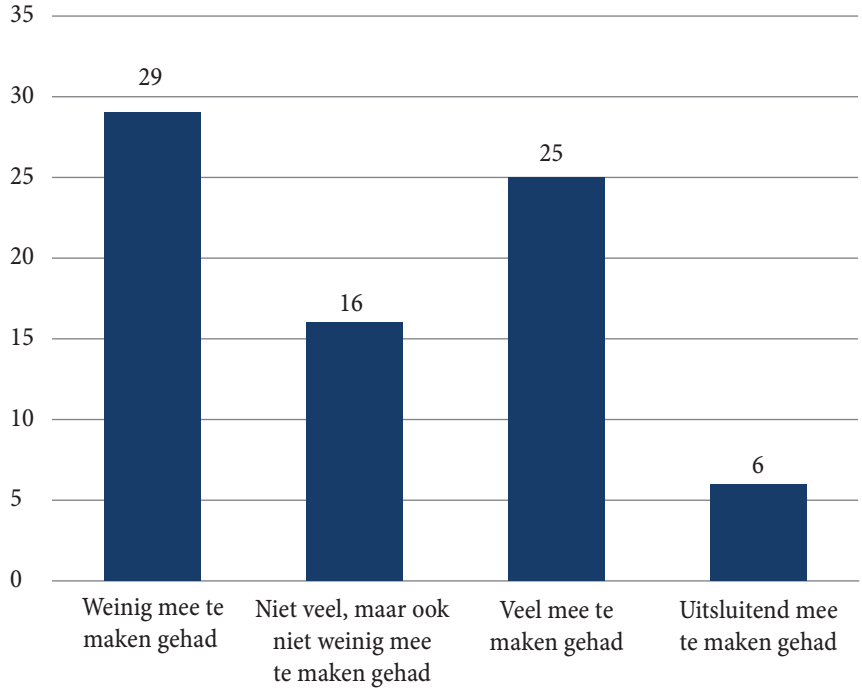
5 Werkzaamheden die eenmaal zijn genoemd zijn: administratief rechercheur districtsrecherche, coördinator rechercheur/recherchekundige, digitaal specialist bij de Regionale Recherche, financieel rechercheur bij de districtsrecherche, gedetacheerd bij het Cybercrime Team als tactisch rechercheur, senior Intake en Service, operationeel specialist digitaal bij Team Digitale Opsporing en operationeel expert wijk thema.

helemaal geen opleiding of cursus te hebben gevolgd op het gebied van digitale criminaliteit. Twaalf respondenten hebben een opleiding/cursus gevolgd op het gebied van zowel cybercrime als gedigitaliseerde criminaliteit, negen alleen op het gebied van gedigitaliseerde criminaliteit en zes alleen op het gebied van cybercrime. Andere opleidingen of cursussen die werden genoemd zijn: iRN (N=7), Open Source Intelligence (OSINT; N=2), DCS-cursus, digitale bewustwording, enkele colleges gevolgd over cybercrime/digitaal, aparte opleiding op het gebied van IT en enkele themadagen gevolgd over cybercrime/digitaal. De laatste vijf opties zijn slechts eenmaal genoemd.

Gemiddeld volgden de respondenten 6,3 opleidings- en/of cursusdagen op het gebied van digitale criminaliteit. Eén respondent volgde honderd opleidings- en/of cursusdagen; het hoogste aantal. De mediaan ligt op drie opleidings- en/of cursusdagen.

Grafiek 3.1 geeft weer in hoeverre de respondenten ervaring hebben met digitale sporen. De respondenten hebben allemaal enige ervaring met digitale sporen, al hebben 29 er weinig mee te maken gehad. Zes respondenten hebben uitsluitend met digitale sporen te maken gehad.

Grafiek 3.1: Ervaring met digitale sporen (N=76, in aantallen)



3.5 Vragenlijst

Na afloop van het casusonderzoek is (digitaal) een korte vragenlijst afgenomen. Naast algemene kenmerken (geslacht, leeftijd, etc.) zijn hiermee kennis en vaardigheden over digitale sporen in kaart gebracht. De vragen zijn gebaseerd op het onderzoek 'Level Up!' dat is uitgevoerd door de onderzoeksgroep Cybersafety en dat gaat over welke kennis politiemensen nodig hebben bij digitale aspecten van criminaliteit (zie bijlage 6).
Daarnaast zijn in de vragenlijst stellingen voorgelegd over de intenties voor het gebruik van digitale sporen. De stellingen zijn geformuleerd op basis van de Reasoned Action Approach (RAA) van Fishbein en Ajzen (2010). Omdat de resultaten mogelijk beïnvloed konden zijn door het casusonderzoek zijn twee weken later dezelfde stellingen voorgelegd middels een online vragenlijst. Bij deze meting werden bovendien de factoren bevraagd die het tactisch gebruik van digitale sporen kunnen belemmeren. Stellingen daarover waren opgesteld naar aanleiding van de interviews (deelvraag 1). Er werden stellingen voorgelegd als: 'Ik ben bang om fouten te maken met digitale sporen'. Aan de tweede vragenlijst deden 54 respondenten mee; een netto retentiegraad van 71,1 procent.
Tot slot werd een maand na deelname aan het casusonderzoek de volgende vraag gesteld: 'In hoeveel procent van de zaken die je de afgelopen maand hebt gedraaid, heb je gebruikgemaakt van digitale sporen?' Dit percentage is gebruikt voor het meten van gedrag (het gebruik van digitale sporen) zodat het verband kon worden getoetst tussen intenties (bevraagd in de tweede vragenlijst) en gedrag. De formulering sluit wederom aan bij de RAA van Fishbein en Ajzen (2010). In totaal hebben 31 respondenten de vraag beantwoord. Een netto retentiegraad van 40,8 procent.

Data-analyse
Voor het analyseren van de opgehaalde gegevens hebben we voornamelijk beschrijvende statistiek toegepast. Daarnaast hebben we een analyse gedaan op doelgroepniveau; daarvoor zijn chi-kwadraattoetsen uitgevoerd. Indien er sprake was van een 2x2 design, is de Fisher's Exact Toets uitgevoerd. Er is steeds gecontroleerd of aan de assumpties van de toets werd voldaan. Bij de beantwoording van deelvraag 3 zijn correlatietoetsen uitgevoerd. Het statistische deel van dit rapport betreft een verkennend onderzoek, gelet op de doelgroep en de aantallen. Daarop wordt in hoofdstuk 8 verder ingegaan.

4. Factoren die het gebruik van digitale sporen belemmeren

4.1 Inleiding

Dit hoofdstuk geeft, aan de hand van literatuur en interviews met zowel experts als politiemedewerkers zonder specifieke kennis van digitale sporen, een eerste overzicht van factoren die er mogelijk voor zorgen dat digitale sporen al dan niet in de opsporing worden gebruikt. In dit hoofdstuk wordt antwoord gegeven op de eerste deelvraag: 'Welke niet-technische factoren belemmeren het tactisch gebruik van digitale sporen door politiemensen?' Het hoofdstuk is ingedeeld in de volgende thema's: (1) kennis, (2) praktische factoren, (3) juridische factoren en (4) mentale factoren. Deze vier thema's komen hierna achtereenvolgens aan bod. We geven steeds eerst een inleiding op het thema aan de hand van literatuur, waarna we bespreken wat in de interviews over het thema naar voren is gekomen. We sluiten elk thema af met een resumé.

4.2 Kennis

De politie geeft prioriteit aan cybercrime en er zijn steeds meer digitaal specialisten in dienst. Wil de politie werkelijk gebruikmaken van digitale sporen, dan is kennis van digitalisering nodig in de volle breedte van de politieorganisatie. Immers, het is zaak dat een politiemedewerker in eerste aanleg de goede waarnemingen doet en de goede maatregelen treft om digitale sporen te kunnen benutten.
Over de volle breedte van de politieorganisatie gezien, is echter sprake van gebrek aan inzicht in digitale mogelijkheden (Stol, Leukfeldt & Klap, 2013; Stol & Strikwerda, 2017). Politiemedewerkers zonder digitale expertise hebben bijvoorbeeld onvoldoende kennis over het uitlezen van gegevensdragers en de internettap, waardoor digitale sporen onzichtbaar blijven (Odinot, Jong & Van der Leij, 2012; Veenstra et al., 2016).
Van Valkengoed (2017) concludeert in zijn surveyonderzoek (N=197) naar digitale kennis onder rechercheurs op verschillende niveaus (regio, district, basisteam) dat zij over onvoldoende digitale basiskennis en basisvaardigheden beschikken. Dit is geen exclusief Nederlands probleem. In het Verenigd Koninkrijk bijvoorbeeld wordt hetzelfde beeld geschetst: "A National Cyber Capabilities Programme assessment of capabilities described low level of skills in the regions to deliver their remit and a very low level of capabilities in local forces" (HMIC, 2014, p. 25-26).

Opleidingen, cursussen en handleidingen kunnen kennistekorten mogelijk verhelpen. Het is dan wel een vereiste dat medewerkers weten waar ze moeten zijn en dat de opgedane kennis beklijft. Flory (2016) ziet in de Verenigde Staten dat er een kennistekort is onder politiemensen, omdat de trainingsmogelijkheden onbekend zijn. In het onderzoek wordt gepleit voor standaardprocedures voor het identificeren, verzamelen en veiligstellen van digitaal bewijs en het opnemen van een trainingsmodule over digitaal bewijs in de basistraining die agenten ontvangen, zodat iedereen een mimimaal vereiste kennis heeft op dat gebied. In Nederland zijn in de periode 2008-2016 een e-learning module ontwikkeld en handreikingen op digitaal gebied. Het effect ervan is evenwel niet onderzocht (Stol & Strikwerda, 2017). In dezelfde periode is in het Verenigd Koninkrijk een e-learning module ontwikkeld om politiemensen digitaal bij te scholen, echter met gering succes: "The average take-up for this training in 37 police forces was less than two percent of staff" (HMIC, 2014, p. 25-26).[6] Hoewel onduidelijk is wat de afzonderlijke inspanningen om de kennis te vermeerderen bij de Nederlandse politie precies hebben opgeleverd, concludeert Van Valkengoed (2017) in zijn hiervoor genoemde onderzoek dat respondenten die een opleiding op het gebied van cybercrime of gedigitaliseerde criminaliteit hebben gevolgd, hoger scoren op zowel digitale kennis als digitale vaardigheden.

Uit de interviews
Eén geïnterviewde benadrukt dat er nu meer dan voorheen aandacht is voor digitaal bewijs.

'Vroeger namen we bijvoorbeeld nooit een spelletjescomputer in beslag, daar kijken we nu wel met andere ogen naar. En pasjes en wallets en noem het allemaal maar op. Alles wat ook maar iets kan bevatten, dat nemen we nu mee of we overleggen dat met de digitaal rechercheur. Dus daar is wel meer aandacht voor.' **(R8)**

Twee andere geïnterviewden zeggen dat politiemedewerkers over dit aspect van het werk nog veel vragen hebben.

'Ik weet niet wat voor informatie je uit routers kunt halen. Daar is in de opleiding ook nauwelijks op afgestemd.' (...) 'De baas heeft mij nooit een cursus gegeven [over social media]. Dus wat ik daar uit kan halen en hoe ik dat kan veiligstellen, ik heb geen flauw idee. Ik weet gewoon echt niet hoe het werkt.' **(R1)**

6 De Scientific Working Group on Digital Evidence (SWGDE) 'brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as ensuring quality and consistency within the forensic community.' De SWGDE richt zich primair op het foutvrij behandelen van digitaal bewijs in een laboratoriumomgeving. In politietermen richt de SWGDE zich dus vooral op de technische behandeling van digitaal bewijs, terwijl onze belangstelling hier uitgaat naar het tactisch gebruik ervan in opsporingsonderzoek. (https://www.swgde.org/about_us, laatst geraadpleegd op 5 november 2019).

'Je hebt echt een heel hoog niveau nodig om je zeker te voelen in die digitale omgeving, dat je de juiste informatie eruit haalt en dat je er echt iets mee kan. En je moet de goede vragen stellen.' (...) 'De huidige generatie jongere politiemensen zijn weliswaar meer opgevoed met de smartphone, maar dat betekent nog niet dat ze begrijpen wat er gebeurt in het apparaat. Ze herkennen in ieder geval de namen van de apps en ze herkennen dat er gechat kan worden in een app, dat is heel fijn. Maar voordat je de technische sporen kan duiden moet je toch meer technische interesse hebben en dat willen uitzoeken en dat is gewoon niet heel veel aanwezig.' **(R2)**

Twee experts plaatsen vraagtekens bij de effectiviteit van opleidingen op digitaal gebied.

'Een van de moeilijkste dingen die altijd horen bij het trainen van mensen en het geven van opleidingen, is de vraag hoeveel beklijft er en hoeveel is je investering waard geweest?' **(R6)**

'Het praktische knelpunt is dus dat wij als organisatie niet goed in staat zijn om kennis aan te bieden op de plekken waar je dat nodig hebt. Op het niveau waarop je het nodig hebt. Eigenlijk bieden we nu helemaal geen kennis aan. Ja, mensen krijgen een training, een opleiding bij de politieacademie en dan drie maanden later, als je ze er dan iets over vraagt, dan zijn ze vergeten wat erin zat.' **(R5)**

Resumé
Uit de literatuur komt het beeld naar voren dat onvoldoende kennis een belemmerende factor kan zijn bij het gebruik van digitale sporen door politiemedewerkers. Hoewel er steeds meer mensen met digitale kennis in dienst zijn gekomen en er inspanningen zijn verricht om politiemensen op dit gebied bij te scholen, is het overall kennisniveau nog onvoldoende. De interviews lijken dat beeld te bevestigen. Een eerste nuancering komt echter van een geïnterviewde die zegt dat er tegenwoordig meer dan voorheen aandacht is voor digitaal bewijs. Een tweede nuancering komt van Van Valkengoed. Hij vindt in een survey onder rechercheurs een positief effect van een opleiding op het digitale kennisniveau van deze politiemedewerkers. We weten weinig over de effectiviteit van opleidingen op digitaal gebied.

4.3 Praktische factoren

Naast het gebrek aan kennis zijn er praktische factoren die het gebruik van digitale sporen kunnen belemmeren. Deze factoren worden achtereenvolgens besproken. Er wordt onder andere ingegaan op een gebrek aan faciliteiten, het versnipperde aanbod van aanwezige kennis en organisatorische aandachtspunten. Er wordt hierna steeds eerst aandacht besteed aan bevindingen uit de literatuur, waarna een vergelijking wordt gemaakt met de interviewresultaten.

Faciliteiten
Volgens eerder onderzoek is er een beperkt aantal uitleesstations beschikbaar om gegevensdragers uit te lezen, net als een beperkt aantal iRN-computers om opsporingsonderzoek op internet te doen (Blaas, 2015).
In de interviews is het algemene beeld van beperkte beschikbaarheid van digitale expertise en iRN-computers niet bevestigd. De geïnterviewde rechercheurs zijn allen werkzaam bij de Eenheid Noord-Nederland, waar het digitaal platform in Leeuwarden is gehuisvest. Over deze benaderbaarheid wordt het volgende gezegd:

'Vroeger kon het echt wel weken duren, dan werd een telefoon via de interne post opgestuurd naar Groningen en dan ging er iemand mee aan de slag. (…) Nu is het zo dat wij de luxe hebben dat ze bij ons zitten en daar ook uitleesstations hebben. Ze zetten het eigenlijk al klaar voor jou op een schijf; die wordt dan ook helemaal apart van de heel andere politiesystemen bewaard. Dus er kan eigenlijk ook nooit mee geknoeid worden. En dan kun je ze gewoon in alle rust uitlezen.' **(R8)**

'*Vroeger zaten [digitaal experts] gewoon ergens verstopt op een afdeling en daar kon je ook niet bijkomen. Ze zaten op een andere locatie en dat is gevoelsmatig ook ver. Dan kan je natuurlijk wel even bellen, maar nu is het gewoon heel makkelijk, met je problemen kun je er naartoe en dan word je ook meteen geholpen. Dus dat is zeker wel een verbetering.'* **(R5)**

Eén geïnterviewde merkt op dat de gebruiksvriendelijkheid een groter probleem is dan de beschikbaarheid van faciliteiten.

'*Het werken met de programma's waarin het spul verwerkt wordt, dat is nog weleens een dingetje. Dat heb je dan een keer gedaan (…) en dan is het programma weer anders of aangepast, nieuwe versie, weet ik veel wat. En doordat je daar niet met grote regelmaat in bezig bent, dan is het toch weleens wat gedoe met zoeken. Maar goed, dan zijn er wel weer mensen die je daar wel mee kunnen helpen.*' **(R9)**

Versnippering van kennis/kennisdeling binnen de organisatie
Uit de literatuur komt naar voren dat samenwerkings- en informatie-uitwisselingsproblemen het gebruik van digitaal bewijsmateriaal kunnen belemmeren (Stol, Leukfeldt & Klap, 2013). Het is vaak onduidelijk aan wie binnen de organisatie een verzoek te richten en de kennis over digitale gegevens is versnipperd aanwezig binnen de organisatie (Veenstra, Zuurveen, Kerstens en Stol, 2015).
In de interviews komt met name het delen van kennis binnen de politieorganisatie als probleem naar voren, bijvoorbeeld bij het gebruik van intranet:[7]

7 ECDO is het landelijke Expertisecentrum Cybercrime en Digitale Opsporing van de politie.

'*Binnen iRN is er zo'n omgeving [waar je kunt] bijhouden welke tooltjes er allemaal zijn voor digitale opsporing. Dat platform hebben we nog niet eens landelijk, elke eenheid doet het op zijn eigen manier. ECDO[7] is een van de manieren om die expertise te bundelen en dat kennismanagement te regelen. Die probeert die kennis door heel het land met elkaar te delen. Maar zij zeggen eigenlijk, wij zijn zo ondergedompeld in de hoeveelheid werk, we komen er helemaal niet aan toe om dat allemaal bij te houden en te delen. Dat komt eigenlijk niet van de grond. Dat is heel jammer, want dat is de enige manier om bij te blijven in je vak.*' **(R2)**

'Hoe intranet werkt, dat weet ik niet helemaal. Je moet heel specifiek je zoekvragen doen en dan ja, hoop je dat je wat naar voren kan toveren waar je verder mee kunt.'**(R8)**

Een aanvullend probleem waar over gesproken wordt in de interviews betreft verouderde en niet up-to-date informatie[8]:

'Ze zouden al dat oude spul wat niet meer van toepassing is op intranet moeten verwijderen na verloop van tijd. Ik heb ook het idee dat dat ook niet altijd gebeurt.' **(R8)**

'We hebben dat KOMPOL, dat is het systeem van de Politieacademie, daar zijn alle oude PolitieKennisNet dossiers een-op-een ingezet. En sindsdien wordt het eigenlijk niet meer onderhouden. (…) Iedereen is gewoon eigen kennispaginaatjes gaan maken, maar dat is niet gecoördineerd. Dus als je als wijkteam hutseknuts een eigen pagina hebt, dan is de kans dat de content die erop staat, de juiste versie en überhaupt zinnig is, eigenlijk niet zo heel erg groot.' **(R5)**

Aard van digitale sporen

Een ander praktisch probleem dat voortkomt uit de literatuur is de vluchtigheid van digitale sporen, waardoor snel moet worden gewerkt om ze te benutten. Door trage besluitvormingsprocessen worden zaken echter te laat opgepakt, waardoor de data al zijn verdwenen en opsporingskansen zijn verkeken (Huisman, Princen, Klerks & Kop, 2016). Ook de (te) beperkte bewaartermijn voor internetverkeergegevens is een knelpunt in opsporingswerk (TRIO Opsporing, 2014). Verder zorgt het internationale karakter van digitale gegevens ervoor dat het vorderen van gegevens vaak bij buitenlandse partijen moet gebeuren, wat erg vertragend kan werken en een taalbarrière kan opleveren (Veenstra et al., 2015; Veenstra et al., 2016). Tot slot kan het moeilijk zijn om IP-adressen te achterhalen door onder andere het gebruik van zogenoemde proxyservers (Veenstra et al., 2015).

Twee geïnterviewden lichten toe op welke wijze de bewaartermijn van gegevens een rol speelt in politiewerk:

8 KOMPOL (Kennis Op Maat Politie) is een systeem voor informatie- dan wel kennisdeling binnen de politie. Zie ook https://www.politieacademie.nl/kennisbank-kompol-vernieuwd.

'Het gebeurt weleens dat je te laat bent. Maar er wordt ook wel een barrière opgeworpen door die providers; soms van, jongens jullie krijgen niet meer dan zoveel maanden, punt. Voorheen kon het wel een jaar, maar dat kan niet meer. Dus dat hebben ze al ingekort. Dan wil je misschien wel meer weten, maar dat krijg je niet.' **(R9)**

'Het ligt een beetje aan de casus. Wij nemen natuurlijk gewoon goederen in beslag waarna we een extractie doen. De bewaartermijn daarvoor is voor ons geen probleem. Wanneer de zaak is afgerond, dan verdwijnt de data achter een slotje en dat is heel logisch, daar hebben wij geen last van op dat moment. Maar ik kan me wel voorstellen dat wanneer bijvoorbeeld iemand zelfmoord heeft gepleegd en uiteindelijk blijkt dat het toch geen zelfmoord is, dat je dan misschien in de knel gaat komen met je bewaartermijn, dat een provider niet meer die data had hoeven te bewaren. Heel eerlijk, voor mij zijn dat de regels van het spel. Bewaartermijn is een horde, dat kan een horde zijn.' **(R10)**

De vertraging door samenwerking met het buitenland (in dit geval met providers) wordt weinig onderstreept in de interviews. Eén juridische expert geeft aan dat het inderdaad een factor kan zijn, ondanks dat er werkafspraken zijn gemaakt met enkele grote partijen. Daarnaast kaart de expert het probleem aan met dynamische IP-adressen:[9]

'De vertraging met het buitenland is er zondermeer. Je zal in heel veel onderzoeken te maken krijgen met buitenlandse providers waarvan de grote vijf natuurlijk snel in beeld komen. Daar hebben we werkafspraken over gemaakt, met die grote vijf. Maar dat wil niet zeggen dat het dan heel soepel loopt. Het blijft worstelen. Op het moment dat law enforcement komt, hebben ze te veel mogelijkheden om te zeggen: deze data mogen we jullie niet geven' **(R6)**

'Heel veel van die IP-adressen in Nederland zijn dynamische IP-adressen. En dan kom je niet verder want KPN kan je al niet van een dynamisch IP-adres vertellen welke smartphone dat was, op dat moment. Dus dat zit 'm in techniek, deels. En daar hebben we geen directe oplossing voor.' **(R6)**

Aanvullend komt in de interviews naar voren dat de overvloed aan informatie een knelpunt kan zijn bij het onderzoek naar digitale sporen. Deze overvloed zorgt tegelijkertijd voor een hoge werklast:

'*Vooral die nieuwere telefoons en de bulk aan gegevens die je krijgt, dat nekt ons soms. Want ja, er staat heel veel in. Dan moet je gaan schiften, wat is wel en [wat is] niet belangrijk? En dat kost veel tijd. Soms moet je gewoon die hele telefoon doorspitten. Dan zijn ze twee, drie, vier dagen bezig met één telefoon. En dan moet het nog op papier komen hè. Als jij te maken hebt met een verdachte die een zaak bekent en ik heb een getuige die zegt*

9 Met de 'grote vijf' in het citaat wordt bedoeld: Apple, Google, Microsoft, Amazon en Facebook.

van ja, ik heb gezien dat die verdachte dat strafbare feit heeft gepleegd. Dan is de zaak rond en heb je die telefoon niet nodig. Maar op het moment dat je een verdachte hebt van, politie zoek het maar uit, nou dan moet je dus op zoek naar andere bewijsmiddelen en dan komt die telefoon misschien wel in beeld.' **(R1)**

'Je moet keuzes maken. Je moet van tevoren bepalen: wat is belangrijk en hoe kunnen we de waarheid aan de dag brengen. Je wilt ook een keer gaan stoppen, je wil ook een keer durven zeggen van we hebben voldoende. En dat gebeurt nog te weinig. Toevallig gisteren ook weer zo'n onderzoek. Dat is al helemaal rond en dan komen ze nog daarna, kan je dit ook onderzoeken? Bij een smartphone, maar je hebt alles al. Want dan willen ze dat het een plusje is, zijn ze extra zeker bij het OM en bij de rechtbank, dat ze het zeker weten, kijk, dat hebben we ook nog.' **(R3)**

Organisatorische factoren

Door Custers (2012) worden enkele organisatorische factoren genoemd bij het gebruik van digitale sporen. Zo speelt financiering en budget een belangrijke rol en de aanwezige capaciteit voor innovatie. Aan laatstgenoemde komt men meestal niet toe. In het onlangs verschenen onderzoeksrapport 'Leren van technologisch innoveren' is de vraag beantwoord welke factoren het technologisch innoveren binnen de politie in Nederland bevorderen of belemmeren. Hieruit blijkt dat projecten een doorlopend gebrek aan capaciteit in aantal en kwaliteit van medewerkers ondervinden (Ernst, Ter Veen, Lam & Kop, 2019).

Capaciteit wordt ook in andere studies genoemd als belangrijke factor (Stol, Leukfeldt & Klap, 2013). Uit diverse focusgroepbijeenkomsten in 2015 kwam naar voren dat er met name sprake is van capaciteitsgebrek bij digitaal experts: zij zijn vaak te druk om vragen te beantwoorden van collega's zonder digitale kennis (Veenstra et al., 2015).

Uit onderzoek van Ordinot, Jong en Leij (2012) waarin overwegingen voor het gebruik van de internettap worden besproken, komt naar voren dat capaciteit van het team belangrijk is bij het gebruik van dit arbeidsintensieve opsporingsmiddel. In de praktijk blijkt dat de persoonlijke voorkeuren van een teamleider daarbij een belangrijke rol kunnen spelen.

In de interviews wordt qua organisatorische factoren ook gerefereerd aan de beschikbare capaciteit en daaraan gekoppeld de keuze voor een bepaald specialisme:

'*Heel veel collega's werken in deeltijd. En wat je dan vaak ziet, is dat die collega's een bepaalde specialisatie hebben, bijvoorbeeld verhoor. Dus ze worden ingezet voor een bepaalde verhoorklus. Dan gaan ze, met de beperkte tijd die ze hebben, zich richten op die verhoorklus. Dan zitten ze niet te wachten op een digitale opleiding. Dan denken ze, het is mooi dat ik die opleiding krijg, maar ik ga het niet gebruiken in de praktijk, want mijn kennis wordt gebruikt voor andere dingen.'* **(R1)**

'*Dit vakgebied specialiseert zich steeds meer. De wereld om ons heen wordt steeds complexer, dus ook ons werk wordt complexer en daarmee trek je een gat met de traditionele recherche, want die liften niet mee met die ontwikkelingen. Die blijven achter. Dus dat gat tussen tactiek en specialisme wordt, als je niet uitkijkt, steeds groter. Een soort basale oplossing is het aannemen van meer specialisten, maar er moet meer geïnvesteerd worden om die recherche op niveau te gaan krijgen, dat die ook veel meer digitaler gaan denken. Want dan kan je veel beter die aansluiting vinden. En die aansluiting zit nog niet goed in elkaar.*' **(R3)**

Het overvragen van experts wordt in de interviews sporadisch genoemd als probleem en tegelijkertijd gezien als iets onvermijdelijks. Zo zegt één geïnterviewde:

'Een van de dingen wat ons ook nekt, is gewoon capaciteit. We hebben best wel mensen die er wat meer verstand van hebben, [maar] die gewoon tot over de oren in het werk zitten. Alleen die moeten ook ingepast worden in de tactische dingen en de praktische dingen. Die moeten getuigen horen, verdachten horen. Het komt er ook bij hè, ze kunnen zich niet alleen maar richten op het digitale deel.' **(R1)**

'We hebben laatst een doorzoeking gehad van een woning en dat ging over handel in verdovende middelen en in die woning zijn een aantal telefoons en een aantal tablets in beslag genomen en dan heb je ook nog een aantal simkaarten. Dus daar kwamen we al uit op tien apparaten. Die gaan naar digi en dan zeggen wij tegen digi: 'alsjeblieft, die tien apparaten'. Dan zijn ze al blij dat ze überhaupt een back-up kunnen maken en dat ze die aan ons ter beschikking kunnen stellen.' **(R1)**

Het gebrek aan middelen voor innovatie wordt door de geïnterviewden in dit onderzoek zelden genoemd als probleem. Eén geïnterviewde zegt:

'Het aanpassingsvermogen van rechercheurs is, denk ik, best groot. Iedereen die nieuwe mogelijkheden ziet binnen de recherche, is daar vaak super enthousiast over. Maar in de praktijk is het best taai om te beginnen, dan wel om de eerste te zijn die het doet. Want dan kost het je gewoon heel veel tijd en moeite om het allemaal te doen. Dat is overal natuurlijk zo. Ook bij de politie.' **(R6)**

Resumé

Uit de literatuur komt naar voren dat knelpunten in het gebruik van digitale sporen worden ervaren door een beperkte beschikbaarheid van faciliteiten en te weinig capaciteit. Zo zijn digitaal experts vaak te druk om alle vragen te beantwoorden van collega's zonder digitale kennis. Daarnaast worden knelpunten ervaren in het inschakelen van kennis, bijvoorbeeld doordat deze versnipperd aanwezig is binnen de organisatie. Tevens vormt de aard van digitale sporen een knelpunt: digitale sporen zijn vluchtig en houden zich niet aan landsgrenzen.

Ten dele worden deze bevindingen bevestigd in de interviews. Knelpunten in de zin van beperkte beschikbaarheid van faciliteiten en digitaal experts worden niet door iedereen herkend. Bij de Eenheid Noord-Nederland zijn de geïnterviewden juist erg positief over de toegankelijkheid van het digitaal platform. Wel is de gebruiksvriendelijkheid van software een aandachtspunt. Verder zijn er, zoals ook in de literatuur naar voren komt, belemmeringen qua verouderde, versnipperde informatie op intranet en herkent men de problemen met capaciteit. Tot slot leidt de grote hoeveelheid data die digitale sporen met zich meebrengt veelal tot een praktische belemmering om hiermee aan de slag te gaan.

4.4 Juridische factoren

Er zijn diverse soorten juridische knelpunten bij het gebruik van digitale sporen. In de interviews is aan de geïnterviewden gevraagd in hoeverre zij juridische knelpunten herkennen dan wel ervaren. Alleen aan de geïnterviewde juridische experts zijn knelpunten op detailniveau uit de literatuur voorgelegd. Er wordt in deze paragraaf ingegaan op het raadplegen van open bronnen bij het uitlezen van digitale sporen, de grenzeloosheid van digitale sporen en de angst voor afwijzing van digitale bewijsstukken door het Openbaar Ministerie of rechters.

Open bronnen en het uitlezen van smartphones
In artikel 3 van de Politiewet (PolW) staat de algemene politietaak beschreven. Dit artikel kan breed ingezet worden binnen het uitvoeren van politiewerkzaamheden. Het wetsartikel biedt echter niet altijd een wettelijke basis voor het gebruik van technologie (Ordinot, Jong & Leij, 2012). Alleen geringe inbreuken op de grondrechten van burgers zijn op basis van art. 3 PolW toegestaan.[10]

Als openbare bronnen persoonsgegevens bevatten, dan worden deze beschermd door art. 8 EVRM[11] (Koops, 2012; Stol & Strikwerda, 2018). Op basis van art. 3 PolW mogen politiemedewerkers niet op stelselmatige wijze open bronnen doorzoeken. Daarvoor is een bijzondere opsporingsbevoegdheid vereist (art. 126j WvSv). Met een (herhaalde) zoekactie in open bronnen kan een groot deel van iemands persoonlijke levenssfeer in kaart worden gebracht en dat gaat verder dan een 'geringe inbreuk' op de persoonlijke levenssfeer.

Een ander voorbeeld van grenzen aan digitale opsporingsbevoegdheden zien we bij onderzoek aan een inbeslaggenomen voorwerp. Een voorwerp in beslag nemen en doorzoeken mag wanneer daarmee niet meer dan een beperkte inbreuk op de privacy wordt gemaakt. In het zogenoemde smartphone-arrest oordeelde de Hoge Raad dat het doorzoeken van een smartphone meer is dan een geringe inbreuk op de persoon-

10 HR 20 januari 2009, *LJN* BF5603.
11 Europees Verdrag tot bescherming van de rechten van de mens.

lijke levenssfeer. Dat komt omdat met het uitlezen van een smartphone inmiddels iemands gehele persoonlijke leven in beeld kan worden gebracht (Stevens, 2017). Deze informatie is privacygevoelig en bovendien zeer omvangrijk.

Twee geïnterviewde rechercheurs lijken zich bewust te zijn van het feit dat ze toestemming nodig hebben van de officier van justitie bij diverse opsporingshandelingen met digitale sporen, al zien ze dat niet per se als een belemmering:

'Je zult het eerst [moeten] overleggen met een officier. Kijk, als jij echt dagelijks de Facebook van Pietje bij gaat houden, ja dan zit er wel iets van stelselmatigheid in en dat soort zaken. Daar moet je dus wel rekening mee houden.' **(R9)**

'Vroeger was het zo van laat je telefoon even zien dan kijken we even wie je laatste contact was. En met wie heb je gebeld? En wat voor foto's staan erop? Dus daar loop je wel tegenaan. Maar uiteindelijk kun je de telefoon in beslag nemen en dan vraag je aan een officier of je toestemming krijgt om het ding te bekijken. Dus het is dan uiteindelijk een formaliteit. Op het moment dat het wel van belang wordt, dan moet je wel weer zorgen dat je dat goed op papier hebt staan.' **(R8)**

Een digitaal expert ziet ook voordelen in de strenge eisen die worden gesteld aan het uitlezen van gegevens:

'Enerzijds helpt het ons, want nu wordt er misschien wat beter nagedacht over waarom iets in beslag moet worden genomen. (…) Ik zie heel vaak: ik wil de WhatsApp-geschiedenis, want ze weten dat daar wat in staat. (…) Dus dat maakt wel dat arresten ons weleens helpen in de prioritering, anderzijds kan het ook beperkend werken' **(R10).**

Grenzeloosheid van digitale sporen

Grenzeloosheid van bewijsmateriaal in de digitale wereld kan ook een belemmering vormen voor het gebruik ervan. Waar een regulier bewijsstuk fysiek ergens geplaatst of gelokaliseerd kan worden, is dit met een digitaal bewijsstuk niet altijd het geval. De servers van bijvoorbeeld Instagram en Facebook bevinden zich in de Verenigde Staten. Wanneer een politieambtenaar een verzoek doet tot het inzien van een Facebookaccount, dient dit via een rechtshulpverzoek te gebeuren aan de Verenigde Staten en dat kan tot vertraging leiden.

Ook buitenlandse wetgeving kan een muur opwerpen (Stol, Leukfeldt & Klap, 2013). Smaad of laster wordt in de Verenigde Staten bijvoorbeeld niet gezien als voldoende grond voor het vorderen van gegevens (Veenstra et al., 2015).

Uit de interviews met juridische experts blijkt dat de plek waar informatie zich bevindt soms een grijs gebied is:

'Wanneer een opsporingsambtenaar zich er bewust van is dat hij binnentreedt in een omgeving die niet in Nederland is; die moet dan stoppen met onderzoek doen. Maar we hebben heel veel casussen waarin het gaat over Google of over Telegram, die zich niet op Nederlands grondgebied bevinden of misschien wel in sommige gevallen. (…) Google zegt: we slaan de data zo dicht mogelijk op bij de persoon die de gebruiker is. Maar ja, is dat dan in Nederland? Of is dat toch in Engeland? Of is dat in Ierland? Dat weet je dan dus niet precies. Dat punt komt in de jurisprudentie niet voor.' **(R5).**

Angst voor afwijzing

Een andere factor is de angst voor afwijzing van digitale bewijsmiddelen door het Openbaar Ministerie of de rechtspraak. Custers (2012) noemt deze mogelijke weigering een belemmerende factor in het gebruik van digitale sporen. Een juridische expert zegt daar het volgende over:

'Nee, ik denk dat het niet angst is. Het is wel absoluut een procesrisico wat je inschat en waar je rekening mee houdt. Dus ik heb bijvoorbeeld collega's die zeggen we gaan het bewijs veiligstellen, maar we zetten het bewijsmateriaal apart. We doen daar apart onderzoek naar, zodat [het] voor een rechter als die het wil uitsluiten later, geen invloed heeft op de andere bewijsmiddelen. Vind ik op zich wel een mooie weg voorwaarts. Aan de andere kant denk ik, dat belemmert je ook eventueel in het doen van verder onderzoek. Dus dat zijn echt de afwegingen, hoe veel risico wil je lopen in de zaak.' **(R6)**

Aansluitend op de literatuur geeft een juridisch expert aan dat kennis over digitale sporen van belang is in de volledige strafrechtsketen en een belangrijke rol speelt bij de eventuele (angst voor de) afwijzing van een bewijsstuk. Alleen dan kunnen digitale sporen optimaal worden benut, zonder dat er fouten worden gemaakt in de inschatting van de bewijswaarde van dergelijke sporen:

'Het is meer een onzekerheid. Ja, de rechter en het OM hebben best wel veel kennis nodig en de advocaten ook, om in staat te kunnen zijn om te zeggen dat bepaald digitaal bewijs nergens op slaat. Dus dat gebeurt niet zo heel vaak. Ik heb geen idee in hoeveel gevallen er weleens iets opgeschreven wordt door iemand die onzeker is over zijn eigen kennis, wat eigenlijk niet blijkt te kloppen. Dus ik kan me voorstellen dat er mensen zijn die die angst hebben en dat daardoor niet doen. Ik kan me ook heel goed voorstellen dat er allemaal mensen zijn die het wel doen, omdat ze onbewust onbekwaam zijn. Dus ze weten niet dat ze een verkeerde aanname hebben en dat ze daardoor als ze eenmaal een locatie zien die interessant is, dan vrij snel zeggen, die is daar geweest. Die telefoon is geweest op die plek, want ik zie die plek in die telefoon en het is een logische plek in het kader van het verhaal wat ik in mijn hoofd heb, hoe het allemaal gegaan is. Terwijl ze niet andersom kunnen kijken van, ik zie ineens een locatie, waar komt die eigenlijk vandaan? En hoe zeker is, gezien de bron, dat die telefoon daar dan geweest is?' **(R5)**

Resumé
Vanuit de literatuur komt naar voren dat onderzoek in open bronnen al snel een stelselmatig karakter heeft en dat art. 3 PolW niet volstaat, maar er bijzondere opsporingsbevoegdheden moeten worden ingezet. Daarnaast zijn er sinds het smartphone-arrest meer bevoegdheden nodig indien politiemedewerkers een smartphone willen uitlezen. Door servers in het buitenland, rechtshulpverzoeken en verschillen in wetgeving met andere landen kunnen tevens knelpunten ontstaan bij het gebruik van digitale sporen. Tot slot stelt Custers dat de angst voor afwijzing van een digitaal bewijsstuk een belemmering kan zijn in politiewerk.
Twee geïnterviewde rechercheurs geven in hun antwoorden te kennen dat zij zich bewust zijn van het feit dat ze toestemming nodig hebben van de officier van justitie bij diverse opsporingshandelingen met digitale sporen, al zien ze dat niet per se als een belemmering. Een geïnterviewde digitaal expert ziet ook voordelen: het juridisch proces draagt bij aan prioritering.
Een juridisch expert erkent dat er belemmeringen zijn doordat digitale sporen een grenzeloos karakter hebben. Diezelfde expert stelt daarnaast dat het van belang is dat de gehele strafrechtsketen kennis draagt van digitale sporen, zodat de bewijswaarde goed kan worden ingeschat.
Tot slot wordt in mindere mate herkend dat angst voor afwijzing van een digitaal bewijsstuk een knelpunt is bij politiewerk. Een geïnterviewde juridisch expert ziet het meer als een procesrisico: er moet altijd rekening gehouden worden met de mogelijkheid dat bewijsmateriaal niet wordt geaccepteerd door het Openbaar Ministerie of de rechtspraak.

4.5 Mentale factoren

Naast praktische en juridische factoren, kunnen ook mentale factoren zoals interesse en onzekerheid een rol spelen bij het al dan niet gebruiken van digitale sporen. Mentale factoren zijn van invloed op de ideeën en overtuigingen die politiemensen hebben over de bewijswaarde van een bewijsstuk: in hoeverre het bewijsstuk onderscheid maakt (of kan maken) tussen de schuld en onschuld van de verdachte (Rassin, 2015).

Gebrek aan interesse
Hoewel moderne technologie aantrekkingskracht heeft, worden nieuwe technologische mogelijkheden op de werkvloer lang niet altijd welwillend ontvangen. Uit onderzoek blijkt dat ze eerder leiden tot werkstress en een gebrek aan interesse (Edison & Geissler, 2003; Skogan, 2008). Wordt men voor de keuze gesteld, dan wordt bij voorkeur gekozen voor het bekende in plaats van het nieuwe.

Uit de interviews blijkt dat een gebrek aan interesse zeker een rol kan spelen:

'*Als je een houding hebt van, moeilijk en weet ik allemaal niet hoor, dan gaat het hem niet worden. Dan wordt het niks. We hebben ermee te maken, jongens. Je kunt niet zeggen*

daar sluiten we onze ogen voor, dat wordt moeilijk, ingewikkeld, doen we niet. Zo werkt het niet.' **(R9)**

'Gebrek aan interesse in technologie is er zeker. Die is er bij het overgrote deel van de burgers. Je wil dat het werkt, maar je hoeft niet te weten hoe het werkt. Dan kom je wel op het basisniveau van een rechercheur, je hoeft niet te weten hoe de techniek werkt, maar je moet je wel realiseren wat voor een bewijsmateriaal er allemaal te halen is.' **(R6)**

Leeftijd en veranderbereidheid
Focusgroeponderzoek wijst er op dat de hoge gemiddelde leeftijd van politiemedewerkers ertoe leidt dat zaken met een digitale component vaker blijven liggen (Veenstra et al., 2015). Edison en Geissler (2003) lieten zien dat jongeren meer dan ouderen geneigd zijn nieuwe technologie te omarmen. In paragraaf 4.3 is al benoemd dat het aanpassingsvermogen van politiemensen een probleem kan zijn (Custers, 2012).

Bovenstaande bevindingen uit de literatuur worden deels ondersteund vanuit de interviews. Het niet gebruiken van nieuwe technologieën wordt echter niet alleen geweten aan leeftijd, maar bijvoorbeeld (ook) aan een gebrek aan veranderbereidheid:

'Dan heb je weer de senior die hier zit. En er komt een jonkie, die komt net kijken, die komt met dat digitale spoor. Die krijgt te horen: Jij komt net kijken, jij weet helemaal niet hoe criminelen werken, ik loop al dertig jaar in het vak rond. Mijn buikgevoel zegt dat het zo zit. En jij komt met die harde schijf en ik snap al niet eens wat je allemaal precies gedaan hebt, waar je het vandaan hebt.' **(R2)**

'Vroeger werd er gezegd de oudere collega's die hebben er niks mee en die willen er vooral ver vanaf blijven en de jonge collega's willen juist wel. Nou, het heeft meer te maken met open staan voor veranderingen en dat is nog weleens moeilijk binnen de politie. En dan maakt de leeftijd niet meer uit.' **(R3)**

'Mentaliteit is moeilijk te veranderen. Dat geldt niet alleen voor de politie. Dat geldt voor ons allemaal. Wij moeten zeggen, houd op met tappen en ga andere dingen doen. En dat gaat langzaam, maar het begint wel volgens mij.' **(R6)**

Onzekerheid en angst
Politiemedewerkers kunnen onzeker zijn over het eigen kennisniveau en bang om onderzoeken te verprutsen. Het elkaar niet durven aanspreken op onkunde speelt daarbij een rol (MacNeil, 2015; Huisman et al., 2016).

Uit de interviews blijkt dat men niet zozeer spreekt van angst, maar wel van afhoudgedrag en collega's die voorzichtig zijn:

'Ik kan me dat wel voorstellen, dat mensen toch wat voorzichtig zijn. Over het algemeen, volgens mij, zoekt iedereen dan wel een expert op van jongens, hoe moet ik het aanvliegen, hoe moet ik het gaan doen? Anders geven ze het wel aan: weet ik niet, doe ik niet of kan ik niet.' **(R1)**

'Je ziet bij rechercheurs die zelf weinig digitale kennis hebben vrij veel afhoudgedrag, ik heb het idee dat dat ook komt doordat ze het een beetje eng vinden van, ja, als ik eenmaal zeg dat ik het ga doen, dan moet ik al wel echt iets vinden en als ik het niet kan vinden, maar iemand anders wel, dan ga ik misschien af.' **(R5)**

Erkenning van digitale sporen
Uit de literatuur blijkt dat het gebruiken van digitale sporen kan worden gezien als zonde van de tijd ('drains valuable resources'); tijd die beter aan traditionele sporen gewijd zou kunnen worden. Politiemedewerkers krijgen meer erkenning bij succes met het gebruiken van traditionele sporen, dan digitale sporen (Holt & Bossler, 2012).

Eerstgenoemde wordt in de interviews als achterhaald gezien en niet herkend. Over erkenning zegt een van de geïnterviewde experts:

'Erkenning van digitale sporen loopt al heel lang en daar zijn we nu naar toe aan het werken om dat te verbeteren. Langzaam zie je ook wel de lichtpuntjes ontstaan, dat gaat langzaam de goede kant op.' **(R3)**

Steun van leiding
Tot slot zijn er factoren die het gebruik van digitale sporen vergroten. Digitale sporen worden onder andere eerder gebruikt wanneer er steun van leidinggevenden is om ze te gebruiken (Holt & Bossler, 2012) en wanneer er aanjagers zijn binnen het team die het gebruik van digitale sporen stimuleren (Lewig & Dollard, 2010).

In de interviews wordt herkend dat het kan helpen wanneer leidinggevenden het gebruik van digitale sporen stimuleren, ook voor de bewustwording:

'We hebben ook te maken met het feit dat vanuit de leiding, steeds meer de nadruk gelegd wordt op de mogelijkheden van digitaal, en uiteindelijk doen we ook aan scores en prestatie-indicatoren. Je moet zoveel gedigitaliseerde onderzoeken draaien in je team. Dat helpt al om die bewustwording wat meer boven tafel te krijgen.' **(R3)**

Resumé
Uit literatuuronderzoek blijkt dat het gebruik van digitale sporen kan leiden tot werkstress en een gebrek aan interesse. Vergrijzing kan een knelpunt zijn, net als een gebrek aan aanpassingsvermogen. Daarnaast kunnen politiemedewerkers onzekerheid ervaren over het eigen kennisniveau en bang zijn voor het maken van fouten. Het elkaar niet durven aanspreken op onkunde speelt daarbij een rol. Verder blijkt uit de li-

teratuur dat het gebruiken van digitale sporen wel wordt gezien als 'zonde van de tijd' en er meer waarde wordt gehecht aan het gebruik van traditionele sporen. Steun van de leidinggevenden is een belangrijke stimulans, net als de aanwezigheid van aanjagers binnen een team.
De interviewresultaten bevestigen dat een gebrek aan interesse een rol kan spelen. De geïnterviewden zien in mindere mate leeftijd als belemmerende factor, maar eerder een gebrek aan veranderbereidheid. Angst voor het maken van fouten met digitale sporen wordt ook niet zozeer herkend, maar wel enige voorzichtigheid in handelen.
In tegenstelling tot de literatuur, wordt in de interviews het gebruik van digitale sporen niet gezien als 'zonde van de tijd'. Wel zegt een geïnterviewde dat de volledige erkenning van het type bewijsstuk er nog niet is, maar dat er gaandeweg steeds meer belangrijke stappen worden gezet. Tot slot zijn de geïnterviewden in overeenstemming met de literatuur van mening dat steun van leidinggevenden kan helpen bij het gebruik van digitale sporen.

5. Gebruik van (digitale) sporen

5.1 Inleiding

Dit hoofdstuk beantwoordt de vraag: 'In hoeverre en op welke wijze gebruiken politiemensen digitale sporen bij opsporingsonderzoek?' Het hoofdstuk is overwegend gebaseerd op het casusonderzoek. Paragraaf 5.2 gaat over de opsporingsstrategie van de respondenten, waarbij de keuze tussen digitale en analoge sporen aan bod komt en wordt toegelicht. Paragraaf 5.3 gaat in op de wijze waarop digitale sporen worden gebruikt. In paragraaf 5.4 ten slotte worden de (algemene) ervaringen besproken die respondenten hebben met het gebruik van digitale sporen.

5.2 Keuzes tussen digitaal of analoog

5.2.1 *Tien keuzes tussen digitaal en analoog*

Deze paragraaf gaat over de vraag aan welke opsporingsstrategie medewerkers de voorkeur geven wanneer zij opsporingsonderzoek verrichten en waarom ze voor die strategie kiezen. Er zijn tijdens het casusonderzoek tien keuzes voorgelegd aan iedere respondent (N=76), waarbij door de respondent steeds een keuze werd gemaakt tussen een analoog dan wel digitaal bewijsstuk. Hierna is eerst de keuzeverdeling procentueel weergegeven. Daarna volgt de toelichting die respondenten gaven op hun keuze voor een bepaalde werkwijze.[12] Bij elke keuze staat een tabel waarin de belangrijkste motivaties zijn gepresenteerd. Een keuze wordt afgesloten met een vergelijking tussen groepen. Met het statistische programma SPSS is getoetst of er significante verschillen zijn ($p<0,05$) voor de variabelen geslacht, leeftijdscategorie, ervaring met zaken op het gebied van digitale criminaliteit en opleidings- en/of cursuservaring. Het volledige protocol voor het casusonderzoek staat in bijlage 2. De casus is als volgt:

Eva doet aangifte van zware mishandeling, diefstal van haar telefoon (met braak) en smaad. Eva vertelt dat ze op 14 januari 2019 ruzie kreeg met haar toenmalige vriend Tony. Het was een heftige ruzie waarbij zowel Eva als Tony naar elkaar zouden hebben

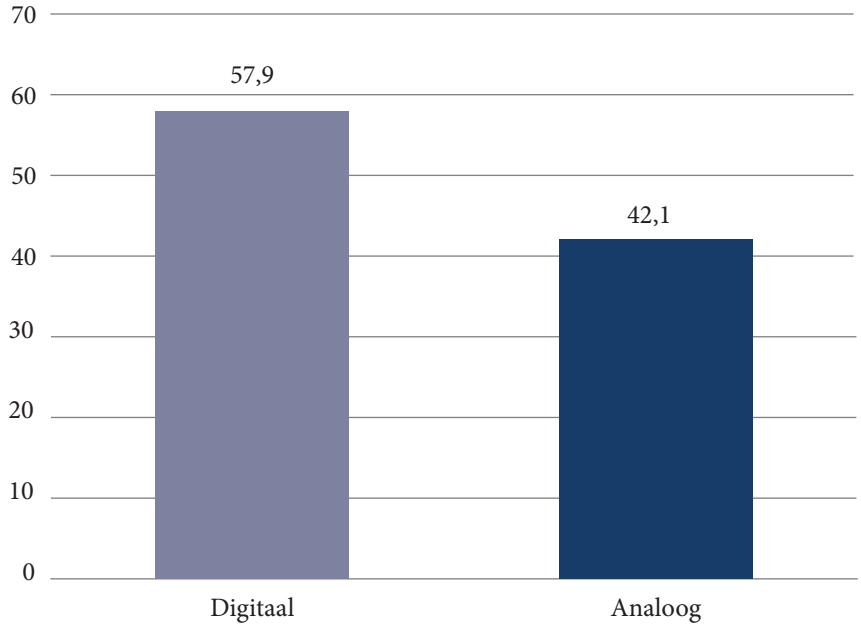
12 De toelichtingen die worden genoemd zijn niet altijd uitputtend voor de gehele groep respondenten, omdat er geen toelichtingen gerapporteerd worden wanneer die toelichting door slechts één respondent is gegeven (een uitzondering daargelaten).

geschreeuwd. Tony zou op een gegeven moment Eva hard in het gezicht hebben geslagen met een hard voorwerp en er vandoor zijn gegaan. Mét haar telefoon, zo bleek later. Eva had als gevolg van de zware mishandeling haar kaak gebroken en moest worden geopereerd.

Zonder toestemming van Eva zou Tony met behulp van haar inlogcode toegang hebben verkregen tot haar telefoon en zou hij een naaktfoto van Eva die op haar telefoon stond op Instagram hebben geplaatst. Tony zou Instagram vervolgens weer hebben uitgelogd, zodat Eva op haar telefoon (toen ze hem weer in beheer had) geen meldingen kreeg over de geposte naaktfoto. Daar moesten haar vriendinnen haar op een later moment op attenderen. Daarnaast zou Tony 500 euro met de ING-app van Eva overgemaakt hebben naar de rekening van ene Henk Elands. Eva vermoedt, onder andere doordat ze weet dat Tony diverse keren is gebeld door andere vrouwen, dat zij niet het enige slachtoffer is.

Keuze 1. De eerste keuzemogelijkheid betrof het raadplegen van de analyseresultaten van (a) de social media-contacten van de aangeefster in haar (openbare) Instagram en Facebookaccounts **(digitaal)** of (b) een buurtonderzoek in de omgeving van de plaats delict **(analoog)**. Drie vijfde van de opsporingsmedewerkers koos voor de analyse van social media-contacten (57,9%), terwijl twee op de vijf (42,1%) koos voor het buurtonderzoek, zie Grafiek 5.1.

Grafiek 5.1: Keuze 1 – Social media of Buurtonderzoek (N=76, in procenten)



Motivatie digitaal bewijs. De 44 respondenten die kozen voor **het onderzoek op social media** deden dat ten eerste omdat ze simpelweg meer waarde hechten aan dit type bewijsstuk (N=33): het kan volgens de respondenten aantonen welke contacten van belang zijn: *"in de buurt zijn niet zoveel contacten, dat gaat nu via social media"* (N=10), wie de dader is van het verspreiden van de naaktfoto's (N=4), wat de tijdlijn is (N=4), wie de naaktfoto's online hebben gezien (N=2) en welke slachtoffers er nog meer zijn (N=2). Eén respondent merkte op: *"data liegt niet"*.

Negen respondenten gaven aan dat het feit dat de casus zich in de digitale wereld afspeelt voor hen de reden is om voor dit digitale type bewijsstuk te kiezen. Twee respondenten zijn vanuit de aard van hun werk 'digital minded', wat ze als argument aanvoerden om voor dit type bewijsstuk te kiezen. Twee respondenten gaven aan dat tijdsdruk een factor is: *"Het is belangrijk dat die gegevens zo snel mogelijk worden veiliggesteld"*. Tot slot merkte één respondent op dat het fysieke gevolg voor het slachtoffer (kaakbreuk) kan herstellen, maar dat de online effecten langer merkbaar kunnen zijn; de naaktfoto verwijderen heeft daarom prioriteit.

Aan de groep respondenten die de voorkeur gaf aan het digitale bewijsstuk werd ook de vraag gesteld waarom ze niet kozen voor het buurtonderzoek (analoog). Hierop werd geantwoord dat een buurtonderzoek, gelet op de casus, niet veel zal opleveren, omdat het niet in de openbare omgeving is gebeurd, maar in de huiselijke sfeer: *"Het meeste is binnen gebeurd, dus buurtonderzoek heeft weinig zin"*. De verwachting is dat het weinig bewijs oplevert: *"smaad ga je hier niet mee aantonen"*. Ook werd opgemerkt dat een buurtonderzoek bewerkelijk is en de keuze voor het digitale bewijsstuk daarom een tijd/capaciteitsafweging is.

Motivatie analoog bewijs. Er zijn 32 respondenten die hebben gekozen voor **het buurtonderzoek**. De waarde van dit bewijsstuk werd gezocht in het feit dat het getuigen kan opleveren van de ruzie (N=11), het de verdachte op de plaats delict kan plaatsen (N=4) en het een eerste indruk geeft van hetgeen er precies heeft plaatsgevonden (N=2). Tot slot gaven twee respondenten aan dat het direct iets oplevert.

Mishandeling werd door negen respondenten als het delict gezien dat in dit geval eerst aandacht moet krijgen. Daarnaast is het een tijdkwestie: enerzijds omdat getuigen details kunnen vergeten en anderzijds omdat er inmenging kan plaatsvinden tussen buurtbewoners (N=4). Tot slot zei één van de respondenten: *"[Het buurtonderzoek is] het meest voor de hand liggend, dat doen we altijd na een incident zoals huiselijk geweld"*.

De respondenten die de voorkeur gaven aan het buurtonderzoek, hebben niet gekozen voor het digitale bewijsstuk omdat het digitale onderzoek volgens hen later ook nog wel kan (N=14) en zij niet inzien wat het kan opleveren over het gepleegde feit (N=6) of over de verdachte (N=2). Daarnaast richt het zich niet op de mishandeling: *"het zwaarste feit"* (N=3). Volgens één respondent is de tijdsduur een factor: *"Het duurt*

langer voordat [verdachte] Tony is aangehouden voor mishandeling. Hoe meer tijd ertussen is, hoe meer aannemelijk het is dat iemand anders aan die telefoon heeft gezeten". Tot slot gaf één respondent aan dat een buurtonderzoek nu eenmaal "*moet gebeuren*" .

Tabel 5.1 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 1. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

Tabel 5.1: Overzicht belangrijkste motivaties keuze 1

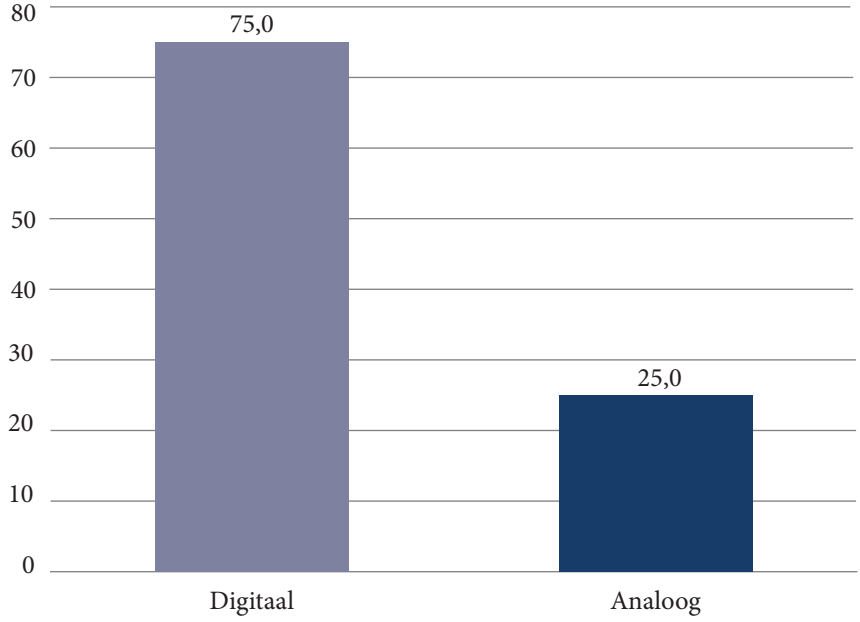
Belangrijkste motivaties keuze digitaal	**Belangrijkste motivaties keuze analoog**
Inzicht in belangrijkste contacten	Mogelijke getuigen van de ruzie
Inzicht in daderschap	Focus op 'offline' mishandeling (in tegenstelling tot online smaad)
Inzicht in tijdlijn	

Verschillen tussen groepen. Er zijn geen significante verschillen tussen mannen en vrouwen in hun keuze voor het digitale dan wel analoge bewijsstuk (p=.629[13]). Ook zijn er geen significante verschillen tussen leeftijdscategorieën (p=.076) en tussen de groepen voor wat betreft ervaring. Tot slot is gevraagd naar het aantal opleidings- en/of cursusdagen dat is gevolgd op het gebied van digitale criminaliteit. Ook tussen deze categorieën zijn geen significante verschillen gevonden (p=.413) (zie ook bijlage 5).

Keuze 2. In het tweede keuzemoment ging het om een afweging tussen (a) open bronnenonderzoek (social media, fora, YouTube, etc.) op de nickname van verdachte **(digitaal)** en (b) een keuze voor het verhoren van een vriend van de verdachte **(analoog)**. Driekwart van de opsporingsmedewerkers koos voor het digitale bewijsstuk (open bronnenonderzoek) (75%), terwijl een kwart koos voor het verhoor (25%).

13 Fisher's Exact Test.

Grafiek 5.2: Keuze 2 – Open bronnenonderzoek of Verhoor (N=76, in procenten)



Motivatie digitaal bewijs. Naast het feit dat een groot deel van de 57 respondenten die koos voor **het open bronnenonderzoek** verwacht dat dit bewijsstuk hen simpelweg meer oplevert, zagen respondenten de waarde van open bronnenonderzoek doordat het informatie geeft over de contacten van de verdachte (N=13), zijn online gedrag (N=4), eventuele andere slachtoffers (N=3) en wat hij nog meer gepost heeft (N=2). Ook kan het volgens respondenten informatie opleveren dat later gebruikt kan worden tijdens een verhoor met de verdachte (N=5).

Zoeken op een nickname kan volgens één respondent veel opleveren: *"oneindig veel mogelijkheden"*. Respondenten zien het als een nuttig bewijsstuk, omdat het objectiever is dan het analoge alternatief (geen afbreukrisico of verstoring) (N=3) en *"onafhankelijk is van verklaringen"* (N=1). Ook werd tijdsdruk aangedragen als motivatie in verband met de vluchtigheid van onlinegegevens (N=2).

De reden dat deze groep niet heeft gekozen voor het analoge bewijsstuk (het verhoor van een vriend van verdachte), is voornamelijk omdat men vindt dat er nog te weinig informatie beschikbaar is. Het zou daardoor een *"kaal"* verhoor worden. Dat het verhoor uiteindelijk moet plaatsvinden wordt erkend: *"nu nog te vroeg"*, maar dit moet eerst voorbereid worden. Een vriend zou daarnaast subjectief zijn en informatie kun-

nen doorgeven over de zaak aan verdachte: *"Getuige en verdachte kunnen elkaar beïnvloeden"*.

Motivatie analoog bewijs. Negentien respondenten kozen voor **het verhoor van een vriend van verdachte**. Het geeft volgens de respondenten informatie over de verhoudingen en onderlinge relaties (N=5). Een getuige kan volgens drie respondenten een waardevol verhaal vertellen over de zaak en aangeven wat er precies gebeurd is. Daarnaast geeft het informatie dat later kan worden gebruikt als ondersteunend bewijs tegen de verdachte (N=1). Het verhoor moet volgens drie respondenten éérst gebeuren, zodat er geen beïnvloeding is tussen getuigen en er snel meer informatie boven tafel komt. Eén respondent zei hierover: *"Verhoor is een geijkt rechercheonderzoek. Zo werken wij"*. Tot slot merkten twee respondenten op dat ze denken dat dit type bewijsstuk meer oplevert dan een open bronnenonderzoek.

De reden dat deze negentien respondenten niet kozen voor het open bronnenonderzoek, is dat het verhoor als een snellere methode wordt ervaren (*"door het horen van [de vriend van verdachte] krijg ik sneller meer informatie")* en dezelfde informatie als uit het digitale bewijsstuk (ook) tijdens het verhoor zou kunnen worden vergaard. Open bronnenonderzoek vond men verder ongericht en te veel ruis opleveren. Het zou daarnaast later ook nog kunnen: *"Social media ligt vast en is altijd te achterhalen"* of de respondenten verwachtten dat het niet veel zal opleveren. Twee respondenten gaven aan dat ze een keuze moeten maken, maar eigenlijk beide zouden willen kiezen. Eén respondent zei over het open bronnenonderzoek: *"[Dat] doen we eigenlijk nooit"*.

Tabel 5.2 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 2. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

Tabel 5.2: Overzicht belangrijkste motivaties keuze 2

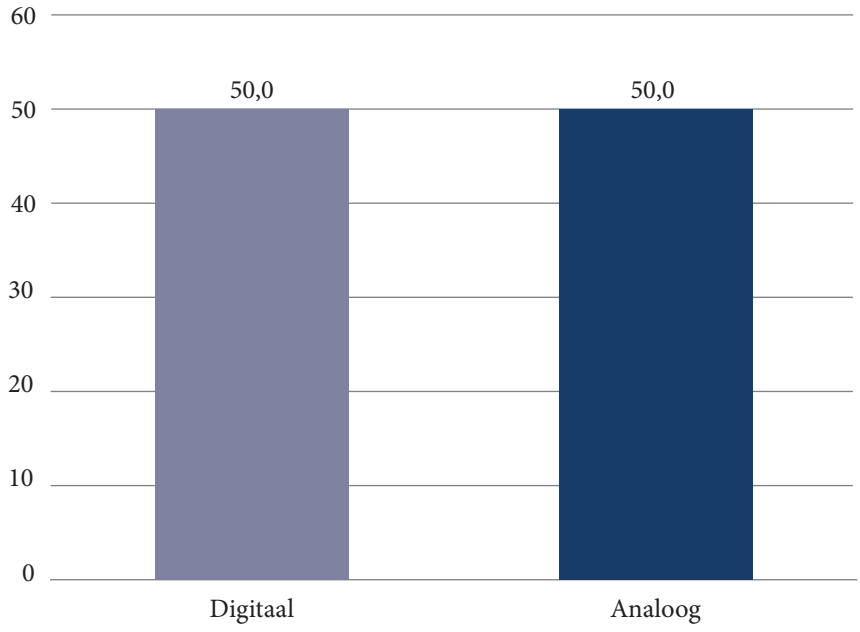
Belangrijkste motivaties keuze digitaal	**Belangrijkste motivaties keuze analoog**
Het levert meer op dan het analoge bewijsstuk	Het levert meer op dan het digitale bewijsstuk
Informatie over contacten verdachte	Informatie over verhoudingen en onderlinge relaties

Verschillen tussen groepen. Er zijn significante verschillen tussen mannen en vrouwen in hun keuze voor het digitale dan wel analoge bewijsstuk (p=.012[14]). 65,3 procent van de mannen kiest voor het digitale bewijsstuk en 34,7 procent voor het analoge bewijsstuk (N=49). 92,6 procent van de vrouwen kiest voor het digitale en 7,4 procent voor het analoge bewijsstuk (N=27). Er zijn geen significante verschillen tussen leeftijdscategorieën (p=.244), ervaring met zaken op het gebied van digitale criminaliteit (p=.204) en aantal opleidings- en/of cursusdagen (p=.347).

14 Fisher's Exact Test.

Keuze 3. Bij de derde keuze werden aan de respondenten de volgende twee opties voorgelegd: (a) het veiligstellen en uitlezen van de modem en router van aangeefster **(digitaal)** of (b) de getuigenverklaring van de overbuurman van aangeefster **(analoog)**. Exact de helft van de opsporingsmedewerkers koos het digitale bewijsstuk (modem en router), terwijl de andere helft de getuigenverklaring als voorkeur had.

Grafiek 5.3: Keuze 3 – Uitlezen modem en router of Getuigenverklaring (N=76, in procenten)



Motivatie digitaal bewijs. De waarde van de sporen wordt gezien in de informatie die het oplevert over wie op welk moment heeft ingelogd op de modem en router (N=22) (*"Deze gegevens zijn keihard"*). Hiermee kan verdachte worden geplaatst op de plaats delict ten tijde van het delict. Een andere motivatie waarom respondenten kozen voor **het uitlezen en veiligstellen van de modem en router van aangeefster** (N=7) ligt in de vergankelijkheid van digitale bewijsstukken. De data zou overschreven kunnen worden. Eén respondent gaf aan dat er informatie kan worden gevonden over of er in het verleden foto's zijn gedeeld met elkaar.

De meerwaarde van het analoge bewijsstuk – de getuigenverklaring van de overbuurman – werd door een groot deel klein geacht (subjectiviteit, buurman moet maar net iets gezien hebben): *"Digitale sporen liegen niet, maar een getuige kan zich vergissen"* (N=16). Zeven respondenten kozen niet voor het analoge bewijsstuk, omdat dat later nog zou kunnen en omdat er geen link werd gezien met de casus. Drie respondenten

hebben eerder voor het buurtonderzoek gekozen (keuze 1) en vonden het daarom niet nodig om nu, voor keuze 3, (opnieuw) de buurman te horen.

Motivatie analoog bewijs. De andere helft van de respondenten koos voor **de getuigenverklaring van de overbuurman van aangeefster**. Redenen voor deze keuze liggen in de focus qua opsporing, namelijk van mishandeling (daar kan een buurman meer over zeggen dan dat wat blijkt uit een modem/router) (N=6), het levert direct/snel bewijs op (N=5) en de meerwaarde qua informatie over feiten en omstandigheden (N=3). Verder werden door vijf respondenten getuigenverklaringen in zijn algemeenheid als belangrijker omschreven (*"Levert meer op"*).

Deze respondenten kozen niet voor het uitlezen van de modem en router, omdat men geen toegevoegde waarde ziet (N=11) of een gebrek aan kennis heeft over hoe dit moet (N=7). Ook werd aangegeven dat dit bewijsstuk op een later moment eventueel kan worden ingezet (N=5). Twee respondenten gaven aan dat specifieke software nodig is om relevante loggegevens uit een modem/router te halen, dus het levert niet per definitie relevante bevindingen op. Daarnaast gaf een respondent aan dat dit onvoldoende zal zijn voor het Openbaar Ministerie: "Die [loggegevens] kunnen niet gehoord worden".

Tabel 5.3 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 3. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

Tabel 5.3: Overzicht belangrijkste motivaties keuze 3

Belangrijkste motivaties keuze digitaal	Belangrijkste motivaties keuze analoog
Informatie over wie op welk moment heeft ingelogd op modem/router	Focus op de 'offline' mishandeling (in tegenstelling tot smaad online)
Vergankelijkheid van de digitale sporen	Getuigenverklaringen leveren meer op
	Direct en snel bewijs

Verschillen tussen groepen. Er zijn geen significante verschillen in hun keuze voor het digitale dan wel analoge bewijsstuk tussen mannen en vrouwen (p=.435[15]), hoeveelheid ervaring met zaken op het gebied van digitale criminaliteit (p=.726) en aantal opleidings- en/of cursusdagen (p=.881). Wel zijn er significante verschillen tussen de leeftijdscategorieën (p=.024). In onderstaande tabel worden de resultaten per leeftijdscategorie weergegeven. De leeftijdscategorie 51 jaar en ouder kiest het vaakst voor een digitaal bewijsstuk met 80 procent, terwijl de categorie 41 tot 50 jaar gemiddeld het minst voor het digitale bewijsstuk kiest met 37,5 procent.

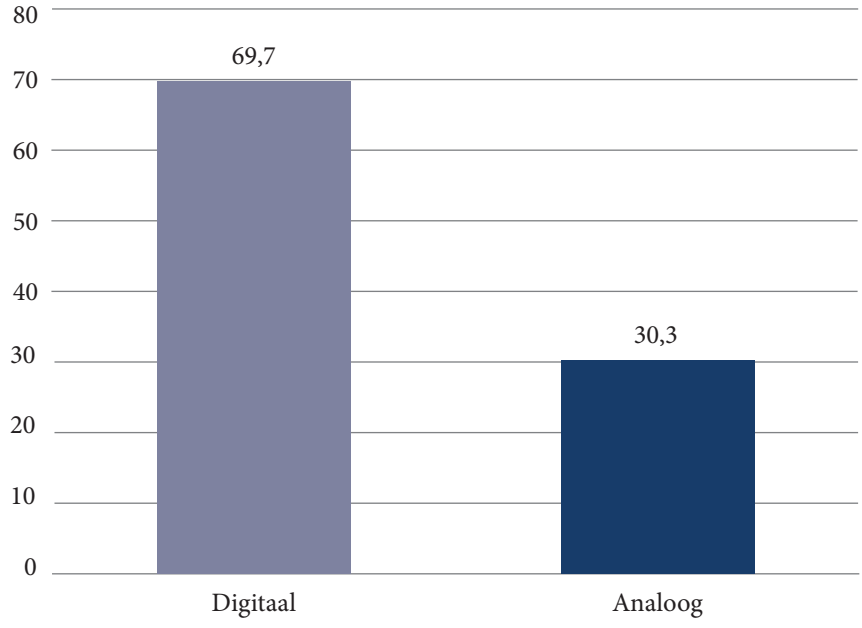
15 Fisher's Exact Test.

Tabel 5.4: Verschillen tussen leeftijdscategorieën (N=75, in procenten)

	Digitaal	Analoog
Tot 30 jaar (N=10)	40	60
31-40 jaar (N=29)	41,4	58,6
41-50 jaar (N=16)	37,5	62,5
51 jaar en ouder (N=20)	80	20

Keuze 4. De **digitale** vierde keuze was (a) een geluidsopname op de smartphone van de buurvrouw van aangeefster ten tijde van het toebrengen van het letsel aan aangeefster. Het **analoge** bewijsstuk (b) betrof de verklaring van een arts over het letsel van aangeefster. Ruim twee derde koos voor de geluidsopname (69,7%), terwijl iets minder dan een derde van de respondenten de voorkeur gaf aan de verklaring van de arts (30,3%).

Grafiek 5.4: Keuze 4 – Geluidsopname smartphone of Verklaring arts (N=76, in procenten)



Motivatie digitaal bewijs. De 53 respondenten die kozen voor **de geluidsopname van de buurvrouw van aangeefster** zien bewijswaarde in de mogelijkheid dat namen en stemmen worden genoemd op de opname, zodat een verdachte op een bepaald tijdstip op de plaats delict kan worden geplaatst (bewijs van daderschap) (N=16). Ook wat er

precies is gebeurd en informatie over de sfeer en context van het delict kunnen mogelijk nuttig zijn volgens vijftien respondenten: *"Duidelijk horen dat er ruzie is en hij haar slaat of zegt waar hij mee slaat"*. De vluchtigheid van dit bewijsstuk werd ook genoemd als argument (N=10): *"Digitaal vervliegt heel snel"*. Drie respondenten gaven aan dat ze de opname willen gebruiken om aanknopingspunten te vergaren om de verdachte te horen.

Het medisch beroepsgeheim werd als struikelblok genoemd om niet voor de verklaring van de arts te kiezen. Het analoge bewijsstuk *"Komt later wel"*. Daarnaast zou de arts niets kunnen zeggen over de dader, op welk moment aangeefster gewond raakte en de toedracht. Het zou volgens deze respondenten enkel een beschrijving van het letsel opleveren, wat middels de casus al bekend is. Meerdere respondenten noemen het verplicht, dus *"die kun je later ook wel krijgen"*.

Motivatie analoog bewijs. In totaal hebben 23 respondenten gekozen voor **de verklaring van de arts**. Twaalf respondenten vonden dat de bewijskracht ligt in de details die de arts kan geven over het letsel, bijvoorbeeld over hoe het letsel tot stand is gekomen. In de toelichting werd ook aangegeven dat deze verklaring verplicht is, dus dat het feitelijk geen keuze is (N=6). Ook werd dit type bewijsstuk officiëler, duidelijker en zwaarwegender genoemd (N=4) dan het digitale bewijsstuk. Eén respondent zei dat het in de rechtbank meer waarde zal hebben dan een geluidsopname: *"Als het een filmopname was geweest, had ik daarvoor gekozen"*.

Er werd door deze groep niet gekozen voor het digitale bewijsstuk, omdat wederom het verplichtende karakter van de verklaring van de arts zou dwingen om te kiezen voor het analoge bewijsstuk. Daarnaast werd genoemd dat een geluidsopname niets zegt over wat er precies is gebeurd, omdat het enkel geluid betreft.

Tabel 5.5 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 4. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

Tabel 5.5: Overzicht belangrijkste motivaties keuze 4

Belangrijkste motivaties keuze digitaal	Belangrijkste motivaties keuze analoog
Plaatsen verdachte op pd ten tijde van delict	Verplicht karakter van bewijsstuk
Informatie over context en sfeer delict	Informatie over details van het letsel
Vluchtigheid van het bewijsstuk	

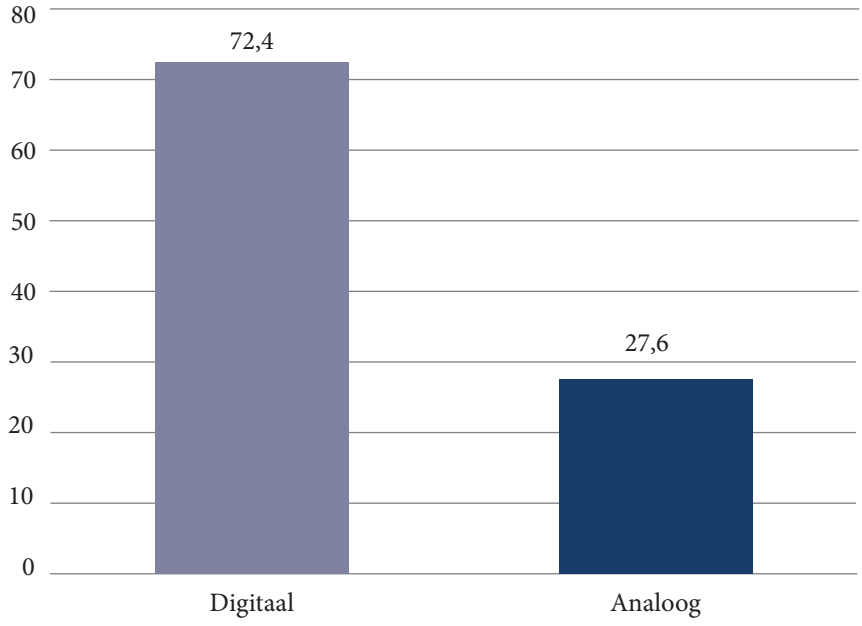
Verschillen tussen groepen. Er zijn geen significante verschillen in hun keuze voor het digitale dan wel analoge bewijsstuk tussen mannen en vrouwen (p=.435[16]). Ook zijn er

16 Fisher's Exact Test.

geen significante verschillen tussen de leeftijdscategorieën (p=.094), de hoeveelheid ervaring met zaken op het gebied van digitale criminaliteit (p=.991) en het aantal opleidings- en/of cursusdagen (p=.837).

Keuze 5. Bij de vijfde keuze konden respondenten kiezen voor (a) het verzoek tot het monitoren van het Instagramaccount van verdachte **(digitaal)** of (b) het verzoek tot observatie van verdachte **(analoog)**. Bijna driekwart koos voor het monitoren van Instagram (72,4%), terwijl iets meer dan een kwart van de respondenten de voorkeur gaf aan het verzoek tot observatie (27,6%).

Grafiek 5.5: Keuze 5 – Verzoek tot monitoren Instagram of Verzoek tot observatie verdachte (N=76, in procenten)



Motivatie digitaal bewijs. Van de 55 respondenten die kozen voor het verzoek tot het monitoren van het Instagramaccount van verdachte, gaven 22 als reden voor deze keuze dat het kan helpen om zijn social media-activiteiten op Instagram in kaart te brengen (zoals het plaatsen van foto's en reacties), ook gelet op eventuele andere slachtoffers. Het zou ook gemakkelijker zijn om in te zetten dan de analoge keuze voor observatie (N=12): *"Minste inbreuk op zijn persoonlijke levenssfeer"*. Daarnaast kan het helpen bij onderzoek naar de locaties die de verdachte heeft bezocht (N=5). Drie respondenten vonden dit de meest geschikte keuze, omdat het delict zich (grotendeels) online afspeelt (N=3). Het levert simpelweg meer op (N=3). Eén respondent zei: *"Het*

lijkt erop dat [verdachte] Tony zich in de fysieke wereld anders gedraagt dan in de digitale wereld […] Ik wil weten wat zijn digitale handel en wandel behelst".

Er werd niet gekozen voor het analoge bewijsstuk, omdat men bang is dat toestemming voor het inzetten van het observatieteam niet gaat lukken. Het is een zwaar middel om in te zetten, ook gelet op de inbreuk op de privacy van verdachte. Respondenten vonden het eveneens niet nodig, omdat het delict zich online afspeelt en er al informatie is over de verdachte als persoon en de locatie van het delict.

Motivatie analoog bewijs. 21 respondenten kozen voor het verzoek tot observatie van verdachte. Ze zien de waarde van dit bewijsstuk vooral in dat het inzicht kan geven in met welke personen hij omgaat (N=9) en zijn gedrag (N=8). Twee respondenten verwachtten dat het online profiel geen betrouwbaar beeld geeft: *"Op Instagram is wat hij zelf wil wat er geplaatst wordt, fysiek heeft hij geen keuze in wat wij zien*". Ook gaf één respondent aan dat hij geen idee heeft hoe het monitoren van Instagram moet worden gerealiseerd.

Tabel 5.6 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 5. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

Tabel 5.6: Overzicht belangrijkste motivaties keuze 5

Belangrijkste motivaties keuze digitaal	**Belangrijkste motivaties keuze analoog**
Inzicht in social media-activiteiten	Inzicht in het gedrag van verdachte
Gemakkelijker om in te zetten	Inzicht in de contacten van verdachte
Inzicht in locaties die verdachte heeft bezocht	

Verschillen tussen groepen. Er zijn geen significante verschillen tussen mannen en vrouwen (p=.433[17]), hoeveelheid ervaring met zaken op het gebied van digitale criminaliteit (p=.356) en aantal opleidings- en/of cursusdagen (p=.496). Wel zijn er significante verschillen tussen de leeftijdscategorieën (p=.023). Per leeftijdscategorie staan in onderstaande tabel de resultaten. De leeftijdscategorie 51 jaar en ouder kiest het vaakst voor een digitaal bewijsstuk met 90 procent. Tot 30 jaar kiest gemiddeld het minst voor het digitale bewijsstuk (40 procent).

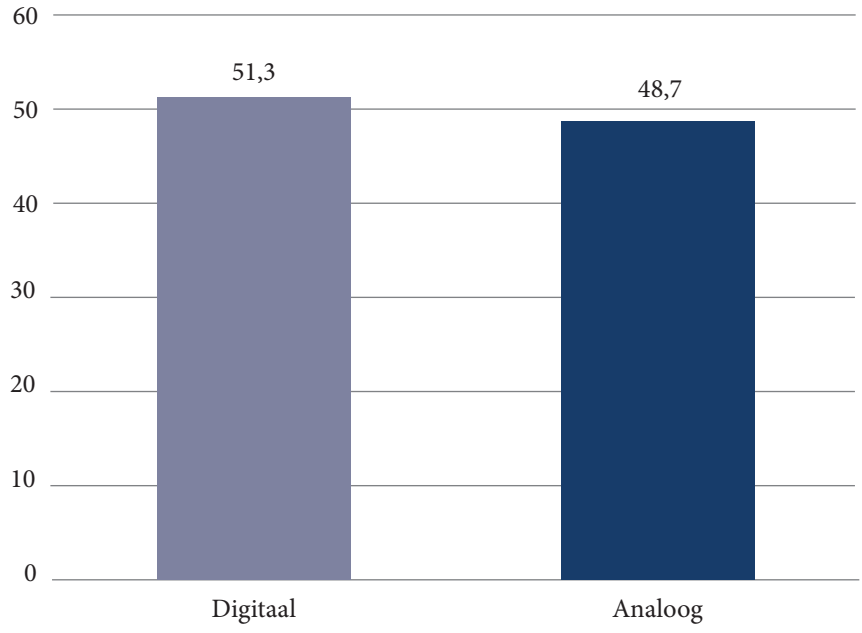
17 Fisher's Exact Test.

Tabel 5.7: Verschillen tussen leeftijdscategorieën (N=75, in procenten)

	Digitaal	Analoog
Tot 30 jaar (N=10)	40	60
31-40 jaar (N=29)	65,5	34,5
41-50 jaar (N=16)	81,3	18,7
51 jaar en ouder (N=20)	90	10

Keuze 6. Vervolgens werd de keuze voorgelegd voor (a) het inzien van de loggegevens van de bank-app van de mogelijke katvanger **(digitaal)** of (b) de resultaten van een verhoor van deze mogelijke katvanger **(analoog)**. Iets meer dan de helft van de opsporingsmedewerkers koos voor de loggegevens (51,3%). De overige respondenten kozen voor het verhoor (48,7%).

Grafiek 5.6: Keuze 6 – Loggegevens of Verhoor (N=76, in procenten)



Motivatie digitaal bewijs. Er zijn 39 respondenten die de voorkeur gaven aan het inzien van de loggegevens van de mogelijke katvanger. In de casus wordt aangegeven dat met de telefoon van aangeefster geld is overgeboekt naar de mogelijke katvanger. Respondenten gaven aan dat ze met het inzien van de loggegevens van de bank-app inzicht willen krijgen in de bevestiging dat die persoon daadwerkelijk het geld heeft ontvangen

(N=7) en wat verder de geldstromen zijn (N=18). Een andere motivatie voor de keuze voor digitale sporen lag in de voorbereiding op het verhoor (N=6). Het wordt gekwalificeerd als feitelijk materiaal (N=5): "Dit liegt niet en een verdachte wel". Het zou daarnaast inzicht geven in de tijdlijn (N=3) en het IP-adres van de mogelijke katvanger (N=2). Twee respondenten maken de koppeling met pingedrag, wat kan leiden tot camerabeelden.

Er werd door deze groep niet voor het analoge bewijsstuk gekozen, omdat aan de betrouwbaarheid van de verklaringen van de katvanger wordt getwijfeld. Ook is men bang dat hij niets gaat zeggen (zwijgrecht). Daarnaast zou er nog te weinig informatie beschikbaar zijn over de mogelijke katvanger en zijn status (verdachte of getuige) om een verhoor af te nemen.

Motivatie analoog bewijs. In totaal hebben 37 respondenten voor het analoge bewijsstuk gekozen: het verhoor van de mogelijke katvanger. Uit de casus blijkt dat er geld is overgemaakt naar deze persoon, wat voor respondenten een reden is om in een verhoor daarnaar te vragen/daarmee te confronteren (N=15). Het verhoor geeft daarnaast voor de respondenten inzicht in de link tussen de mogelijke katvanger en verdachte en eventueel met aangeefster (N=4). Het kan helpen om bewijs tegen verdachte te verzamelen (N=2). Overige respondenten gaven aan dat ze hem vragen willen stellen om op die manier meer informatie te verzamelen. Eén respondent gaf als toelichting: *"Je kunt er direct mee aan de slag"*.

Er werd niet voor de loggegevens gekozen, omdat enkele respondenten niet weten wat er mee bedoeld wordt. De toegevoegde waarde werd er niet van ingezien: *"Ik zie geen link met de casus"*. Daarnaast verwacht men niet dat er toestemming voor gegeven wordt. Het verhoor zou net zoveel informatie opleveren, omdat in het verhoor gevraagd kan worden naar de overboeking. Ook werd aangegeven dat het bekijken van die gegevens *"later nog wel kan"*. Het is *"te beperkt"*, *"zijn geen harde gegevens"* en doordat er al informatie is over de overboeking via de rekening van aangeefster, zijn deze gegevens *"niet nodig"*.

Tabel 5.8 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 6. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

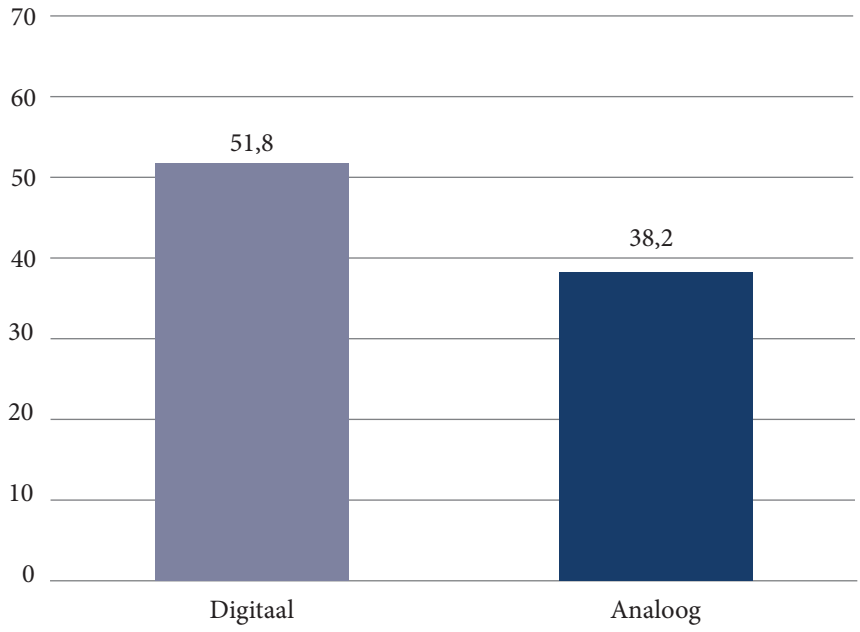
Tabel 5.8: Overzicht belangrijkste motivaties keuze 6

Belangrijkste motivaties keuze digitaal	**Belangrijkste motivaties keuze analoog**
Bevestiging dat geld van aangeefster is ontvangen	Confrontatie met overboeking van rekening aangeefster
Inzicht in geldstromen	Inzicht in link mogelijke katvanger met verdachte en aangeefster
Ter voorbereiding op het verhoor	

Verschillen tussen groepen. Er zijn geen significante verschillen tussen mannen en vrouwen in hun keuze voor het digitale dan wel analoge bewijsstuk (p>.99[18]). Er zijn ook geen significante verschillen tussen leeftijdscategorieën (p=.822), hoeveelheid ervaring met zaken op het gebied van digitale criminaliteit (p=.472) en aantal opleidings- en/of cursusdagen (p=.523).

Keuze 7. De zevende keuze ging tussen (a) belastende berichten afkomstig van verdachte over het delict, die een vriend van verdachte heeft ontvangen op zijn telefoon **(digitaal)** of (b) 'Een tweede slachtoffer van verdachte meldt zich' **(analoog)**. Ongeveer drie op de vijf respondenten koos voor eerstgenoemde (61,8%). De informatie van het tweede slachtoffer werd gekozen door ongeveer twee op de vijf respondenten (38,2%).

Grafiek 5.7: Keuze 7 – Belastende berichten of Tweede slachtoffer (N=76, in procenten)



Motivatie digitaal bewijs. De groep van 47 respondenten die heeft gekozen voor de belastende berichten doet dat met name omdat ze deze vluchtige gegevens zo snel mogelijk willen veiligstellen, ook gelet op het feit dat deze vriend zich kan bedenken (N=7). Het wordt als een concreet, feitelijk bewijsstuk gezien (N=6). Twee respondenten willen op deze manier meer te weten komen over de verdachte. Overige respondenten gaven aan dat het volgens hen meer bewijs oplevert dan het analoge bewijsstuk. Het feit dat een *"vriend wordt verlinkt"* kan volgens één respondent interessante infor-

18 Fisher's Exact Test.

matie opleveren. Overigens vindt een groot deel van de respondenten het een erg lastige keuze. Er wordt aangegeven dat men normaal gesproken voor beide bewijsstukken zou kiezen.

Er wordt niet gekozen voor het analoge bewijsstuk door deze groep, omdat het niet gericht is op de zaak waar men nu aan werkt (met aangeefster en verdachte). Het horen van een tweede slachtoffer zou een nieuwe zaak openen: *"Dat kan later wel"*. Voor nu is het nog onbekend wat het tweede slachtoffer zou opleveren voor deze casus. Respondenten zouden daarnaast te weinig informatie hebben om te kiezen voor het tweede slachtoffer. Men kiest dan liever voor het sterker maken van de zaak die voor hen ligt.

Motivatie analoog bewijs. 29 respondenten hebben gekozen voor het tweede slachtoffer. Respondenten willen aandacht besteden aan een slachtoffer dat zich meldt (N=9): *"Ik vind het belangrijk dat slachtoffers te woord gestaan worden en serieus worden genomen"*. Het zou de zaak daarnaast sterker maken, omdat er meer bewijs over de verdachte wordt verzameld (N=6). Tevens zou het bijdragen aan het bewijzen van stelselmatigheid (N=4). Ook kan het helpen bij het krijgen van vorderingen (N=2). Eén respondent noemt het de *"basis van het werk"* bij de politie. Overige respondenten gaven aan dat ze prioriteit geven aan het tweede slachtoffer en hopen dat hier meer informatie uit komt.

Er werd niet gekozen voor het digitale bewijsstuk, omdat men niet kan inschatten wat het zou kunnen opleveren: *"Het is maar de vraag of ik bij [verdachte] Tony kom"*. Een vriend van de verdachte kan gemanipuleerd zijn. Het slachtoffer vindt men belangrijker. Tot slot wordt aangegeven dat men verwacht dat het andere bewijsstuk meer oplevert. Ook nu gaven respondenten aan voorkeur te hebben om voor beide bewijsstukken te kiezen.

Tabel 5.9 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 7. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

Tabel 5.9: Overzicht belangrijkste motivaties keuze 7

Belangrijkste motivaties keuze digitaal	**Belangrijkste motivaties keuze analoog**
Zo snel mogelijk willen veiligstellen van vluchtige gegevens	Aandacht schenken aan een slachtoffer dat zich meldt
Concreet, feitelijk bewijsstuk	Meer bewijs verzamelen over verdachte
	Aantonen stelselmatigheid

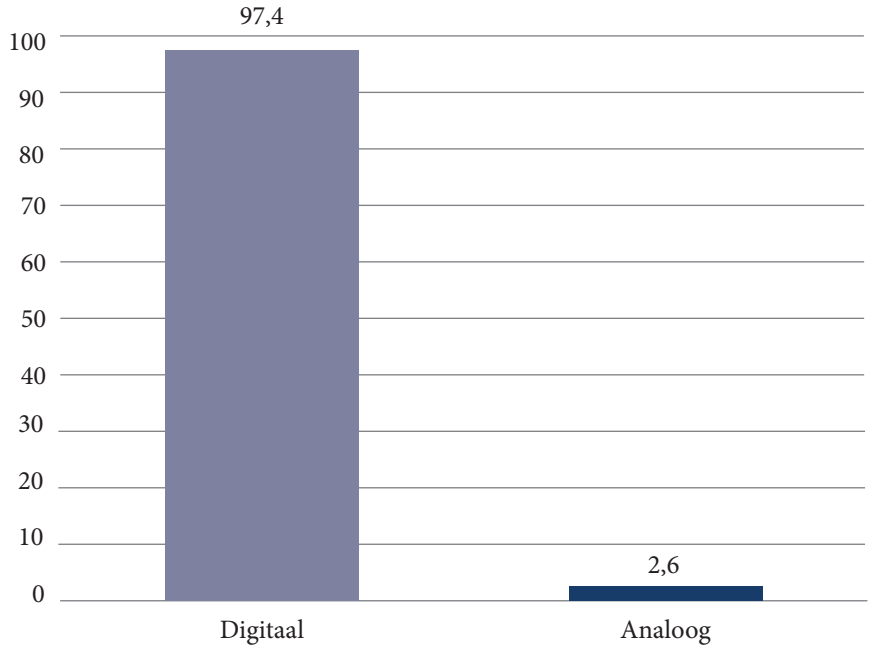
Verschillen tussen groepen. Tussen mannen en vrouwen zijn er geen significante verschillen in hun keuze voor het digitale dan wel analoge bewijsstuk (p=.624[19]). Ook

19 Fisher's Exact Test.

tussen de leeftijdscategorieën zijn er geen verschillen (p=.488), net als tussen de hoeveelheid ervaring met zaken op het gebied van digitale criminaliteit (p=.210) en het aantal opleidings- en/of cursusdagen (p=.563).

Keuze 8. Vrijwel alle respondenten (97,4%) kozen voor de **digitale optie** bij de achtste keuze (a): 18 GB aan data afkomstig uit de uitgelezen telefoon van verdachte, in tegenstelling tot de **analoge optie** (b): dertig dozen met de administratie van verdachte. Slechts twee respondenten kozen voor laatstgenoemde optie (2,6%).

Grafiek 5.8: Keuze 8 – Data of Administratie (N=76, in procenten)



Motivatie digitaal bewijs. De grote groep van 74 respondenten koos voor de 18 GB aan data, omdat het volgens hen simpelweg veel informatie bevat (N=34): *"Hele leven staat op een telefoon"*. Er is interesse in onder andere de foto's, contacten, betaalgegevens, locatiegegevens, (verwijderde) berichten en tijdstippen. Gelet op de casus (die zich deels afspeelt in de digitale wereld) vinden elf respondenten het de beste keuze. Het zou daarnaast gemakkelijker zijn om in te zoeken (N=10), sneller resultaat opleveren (N=8) en actueler zijn (N=5). Eén respondent zei: *"Hoe jonger [verdachte] Tony is, des te waarschijnlijker dat er meer relevante info in de telefoon zit"*.

Er wordt niet voor de dertig dozen administratie gekozen, omdat het veel tijd kost om al die informatie door te spitten, het achterhaald is (*"Dat gaat allemaal heel ver terug"*) en er niet wordt verwacht dat het nuttige informatie oplevert: *"Tegenwoordig heeft nie-*

mand meer administratie". Ook ziet men niet in wat deze administratie met het strafbare feit in de casus te maken heeft. Eén respondent merkte op: "*Tegenwoordig is alles digitaal*".

Motivatie analoog bewijs. Slechts twee respondenten kozen voor de dertig dozen met administratie. De ene respondent koos hiervoor omdat de opsporingsmedewerker inzicht wil in de geldstromen in deze zaak. De andere respondent koos hiervoor omdat er nieuwsgierigheid is naar andere *"louche dingen*", bijvoorbeeld witwaspraktijken.

Deze twee respondenten kozen niet voor het digitale bewijsstuk omdat het geen financiële inzichten zou geven en omdat de administratie interessanter en leesbaarder zou zijn dan het digitale bewijs.

Tabel 5.10 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 8. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

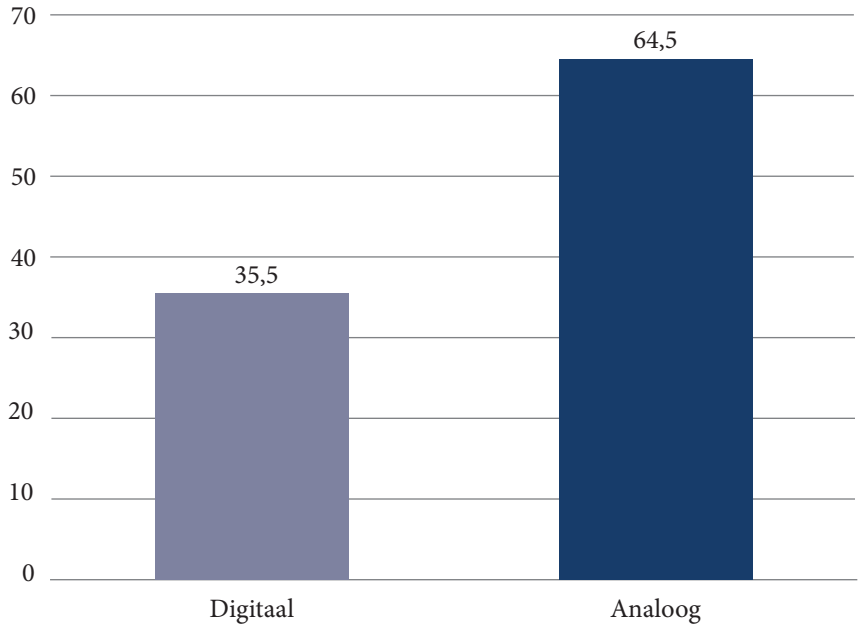
Tabel 5.10: Overzicht belangrijkste motivaties keuze 8

Belangrijkste motivaties keuze digitaal	**Belangrijkste motivaties keuze analoog**
Bevat veel nuttige informatie	Niet van toepassing
Passend bij de casus	
Gemakkelijker om in te zoeken	

Verschillen tussen groepen. Gezien het lage aantal respondenten dat koos voor de analoge optie zijn de verschillen tussen groepen hier niet berekend.

Keuze 9. De negende keuze was ofwel (a) de door de verdachte aangeleverde screenshots van de loggegevens van een game, met profielnaam 'Tonzone' (de nickname van verdachte; **digitaal**) of (b) een door verdachte aangeleverde getuige **(analoog)**. Iets meer dan een derde van de respondenten koos voor de screenshots (35,5%). Ongeveer twee derde gaf de voorkeur aan de aangeleverde getuige (64,5%).

Grafiek 5.9: Keuze 9 – Screenshots of Getuige (N=76, in procenten)



Motivatie digitaal bewijs. De 27 respondenten die hebben gekozen voor het digitale bewijsstuk deden dit omdat het bewijsstuk als betrouwbaarder en/of objectiever/harder wordt gezien (N=9). Respondenten verwachten dat de communicatie tussen personen in het spel (chatgegevens) (N=5) en de profielnaam (N=3) gebruikt kunnen worden voor de zaak. Daarnaast geeft het de mogelijkheid tot het vaststellen van een alibi (N=5). Drie respondenten gaven aan dat het meer zou opleveren dan het analoge bewijsstuk. Overigens werd door elf respondenten genoemd dat het digitale bewijsstuk manipuleerbaar is en verder onderzoek verdient.

Deze respondenten kozen niet voor het analoge bewijsstuk, omdat de getuige mogelijk onbetrouwbaar is, aangezien de getuige is aangeleverd (en mogelijk gemanipuleerd is) door de verdachte. Men verwacht dat de screenshots makkelijker te onderzoeken zijn op eventuele manipulatie, maar de getuige niet.

Motivatie analoog bewijs. Het merendeel van de respondenten koos voor het analoge bewijsstuk (N=49); de door verdachte aangeleverde getuige. Zeven respondenten kozen hiervoor, juist omdat hij vóór de verdachte wil getuigen: *"Je moet alle scenario's open houden"*. Daarnaast zijn respondenten nieuwsgierig naar wat de getuige te zeggen heeft (N=9). Veertien respondenten noemden dat de getuige beïnvloed kan zijn, maar door de getuige te horen kan daar 'doorheen geprikt' worden (vastpraten, doorvragen,

confronteren, controlevragen stellen). Getuigen moeten volgens de respondenten sowieso gehoord worden (N=4) en mogen geen valse verklaring afleggen (N=4). Tot slot gaf men aan dat een getuige meer oplevert (N=3).

Er is onduidelijkheid bij deze groep respondenten over wat loggegevens kunnen opleveren; één van de redenen waarom ze niet voor het digitale bewijsstuk hebben gekozen: *"Screenshots ken en weet ik niet"*. Het bewijsstuk zou gemakkelijk te manipuleren zijn. Daarnaast kan iedereen inloggen met een bepaald account, dat wil niet zeggen dat het de verdachte was: *"Het kan wel iemand in Brazilië zijn"*. Ook wordt genoemd dat de informatie uit dit bewijsstuk niet nuttig dan wel nodig is voor de zaak: *"Ik zie geen relatie met de casus"*. Een getuige zou bovendien meer opleveren voor de waarheidsvinding.

Tabel 5.11 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 9. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

Tabel 5.11: Overzicht belangrijkste motivaties keuze 9

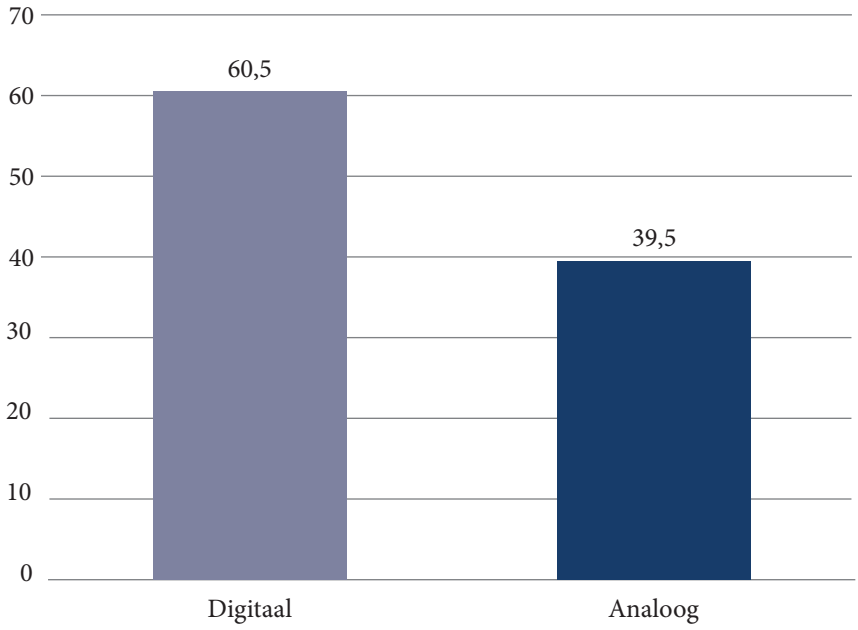
Belangrijkste motivaties keuze digitaal	**Belangrijkste motivaties keuze analoog**
Betrouwbaarder/objectiever	Mogelijkheid tot doorvragen/controle
Inzicht in chatgegevens (communicatie)	Inzicht in ontlastend scenario voor verdachte
Vaststellen alibi	Nieuwsgierig naar verhaal getuige

Verschillen tussen groepen. Er zijn geen significante verschillen tussen mannen en vrouwen in hun keuze voor het digitale dan wel het analoge bewijsstuk ($p>.99$[20]). Tussen de leeftijdscategorieën zijn ook geen significante verschillen gevonden ($p=.616$). Dit geldt ook voor de hoeveelheid ervaring met zaken op het gebied van digitale criminaliteit ($p=.703$) en het aantal opleidings- en/of cursusdagen ($p=.342$).

Keuze 10. Als laatste werd de keuze voorgelegd voor (a) een verkenning van relevante fora op het dark web in combinatie met de nickname van verdachte **(digitaal)** of (b) een TCI-aanvraag (Team Criminele Inlichtingen) over de verdachte **(analoog)**. Ongeveer drie op de vijf respondenten koos voor het onderzoek op het dark web (60,5%), in tegenstelling tot de overige respondenten die kozen voor de TCI-aanvraag (39,5%).

20 Fisher's Exact Test.

Grafiek 5.10: Keuze 10 – Dark web of TCI (N=76, in procenten)



Motivatie digitaal bewijs. Van de 46 respondenten die kozen voor onderzoek op het dark web, deden elf dit omdat naaktfoto's een rol spelen in de casus: *"Verspreidt hij dat? Verwijst hij ernaar? Verkoopt hij dat?"*. Het zou meer informatie opleveren (N=8), bijvoorbeeld over de werkwijze en online gedragingen van verdachte (N=5), zijn alibi (N=3) en zijn netwerk (N=2). Vier respondenten verwachtten informatie te vinden over mogelijke andere slachtoffers (N=4). Tot slot speelt de digitale component in de zaak een rol bij de keuze (N=3) en dat men vindt dat er sneller resultaat kan worden verkregen via het dark web (N=2).

TCI wordt niet gekozen omdat onduidelijk is wat TCI kan doen in deze zaak, ook gelet op het digitale karakter van de casus: *"Je weet niet wat je krijgt, of er info beschikbaar is over [verdachte] Tony en hoe betrouwbaar die informatie dan is"*. Het wordt gezien als een te zwaar middel: *"TCI gaat voor dit soort feiten niet aan het werk"*. Naast dat men niet verwacht veel informatie te krijgen (*"Je moet heel erg mazzel hebben dat [verdachte] Tony met iemand heeft gepraat"*), zou het ook te lang duren totdat die informatie wordt aangeleverd. Ook verwacht men dat dit middel eventueel later nog kan worden ingezet. Tot slot zou een aanvraag niet nodig zijn: *"Als die iets hadden gehad, dan delen ze dat wel´*.

Motivatie analoog bewijs. In totaal hebben dertig respondenten voor het analoge bewijsstuk gekozen. De TCI zou meer informatie opleveren (N=7), bijvoorbeeld omdat het een beeld van de verdachte geeft (N=6). De informatie vanuit TCI wordt betrouwbaarder (N=2), belangrijker (N=1) en concreter (N=1) genoemd: *"Het zijn specialisten"*. Daarnaast kan het informatie geven over mogelijke andere slachtoffers (N=2): *"Veel meiden durven geen aangifte te doen, maar informeren politie op andere manier"*.

Er wordt niet gekozen voor het dark web omdat het verband niet wordt gezien met de casus. Men weet niet hoe het dark web 'werkt' (*"Ik ben allang blij dat ik het gewone internet gebruik"*), wat hier gevonden kan worden en hoe betrouwbaar die informatie is: *"Geen flauw idee wat dit zou opleveren en hoe dit eruit ziet"*. Het zoeken op de nickname van de verdachte wordt door meerdere respondenten als ongeschikte methode gezien: *"Je moet nog maar aantonen dat het om de verdachte gaat"*.

Tabel 5.12 vat de bevindingen samen met een weergave van de belangrijkste motivaties bij keuze 10. De mate van belangrijkheid verwijst naar hoe vaak de motivatie werd genoemd.

Tabel 5.12: Overzicht belangrijkste motivaties keuze 10

Belangrijkste motivaties keuze digitaal	Belangrijkste motivaties keuze analoog
Inzicht in wat met naaktfoto's is gedaan op het dark web	Levert meer informatie op
Levert meer informatie op	Inzicht in verdachte
Inzicht in mogelijk meerdere slachtoffers	Betrouwbaarder, belangrijker, concreter

Verschillen tussen groepen. Er zijn geen significante verschillen tussen mannen en vrouwen in hun keuze voor het digitale dan wel het analoge bewijsstuk (p=.142[21]). Tussen de leeftijdscategorieën zijn ook geen significante verschillen gevonden (p=.639) en ook niet qua aantal gevolgde opleidings- en/of cursusdagen (p=.346). Wel zijn er significante verschillen in de hoeveelheid ervaring met zaken op het gebied van digitale criminaliteit.[22] In onderstaande tabel worden de antwoorden weergegeven. Uit de tabel blijkt dat de respondenten die niet veel, maar ook niet weinig met zaken op het gebied van digitale criminaliteit te maken hebben gehad, vrijwel allemaal kiezen voor het digitale bewijsstuk (93,8%). De groep die uitsluitend dan wel veel met dergelijke zaken te maken heeft gehad, kiest in verhouding het minst voor het digitale bewijsstuk (45,2%).

21 Fisher's Exact Test.

22 In een eerste analyse was de p-waarde .012. Omdat twee cellen in de tabel echter een verwachte waarde ('Expected Count') hadden die lager is dan 5, zijn de categorieën 'Uitsluitend mee te maken gehad' en 'Veel mee te maken gehad' samengevoegd. Dit leidde tot een significant resultaat met een p-waarde van .005.

Tabel 5.13: Verschillen in ervaring met zaken digitale criminaliteit (N=76, in procenten)

	Digitaal	Analoog
Weinig mee te maken gehad (N=29)	58,6	41,4
Niet veel, maar ook niet weinig mee te maken gehad (N=16)	93,8	6,3
Uitsluitend of veel mee te maken gehad (N=31)	45,2	54,8

5.2.2 *Samenhang uitkomst van keuze en opvolgende keuze*

Hoewel geen expliciet onderdeel van ons onderzoek, is het mogelijk dat negatieve output op een keuze (analoog/digitaal) van invloed is op de volgende keuze (analoog/digitaal). Om hier iets over te kunnen zeggen, hebben we vier situaties geanalyseerd. Dit betreft de tweede, de vijfde, de zesde en de achtste keuze (zie bijlage 2). Bij deze vier keuzes was de ervaring van de keuze negatief. Omdat het om een aanvullende, verkennende analyse gaat – we hebben immers maar één experimentele conditie – zijn de keuzes bij elkaar opgeteld.

Van de zojuist genoemde keuzemogelijkheden werd 225 keer voor het digitale bewijs gekozen en 79 keer voor het analoge bewijsstuk. Van de personen die het digitale bewijs kozen, koos daarna 53,3 procent voor het analoge bewijs. Van de personen die het analoge bewijs kozen, koos daarna 58,2 procent voor het digitale bewijs. Er is geen sprake van significante verschillen (p=.45). Het lijkt er op basis van dit onderzoek dus niet op dat een negatief resultaat op een keuze het verloop van de opvolgende keuzes heeft beïnvloed. Vervolgonderzoek is echter nodig om hierover meer zekerheid te verkrijgen.

Uit de open antwoorden op de vraag 'Heeft het resultaat van ieder bewijsstuk invloed gehad op de daaropvolgende keuze?' kwam naar voren dat 27 respondenten zeiden wél door een bepaald resultaat te zijn beïnvloed en 42 respondenten niet (bijlage 2 geeft een overzicht van de keuzes en de daaraan verbonden resultaten). Zeven respondenten gaven een ander antwoord. Slechts een deel van de respondenten gaf een toelichting op het antwoord. Respondenten die zeiden *niet* beïnvloed te zijn, gaven aan dat iedere keuze apart werd bekeken, ongeacht het resultaat van de vorige. De overige antwoorden (zonder een duidelijke ja/nee) hielden in dat er soms wel, soms niet sprake was van beïnvloeding of dat het totaalplaatje op dat moment in de casus bepaalde welke keuze werd gemaakt. In tabel 5.14 staan de gegeven toelichtingen van wanneer men zei wél beïnvloed te zijn:

Tabel 5.14: Toelichting waarom men zegt wel beïnvloed te zijn door resultaat bewijsstuk

Met name door een negatief resultaat. Dan de keuze voor bewijsstuk dat verder afligt van vorige keuze.
Nadat verdachte op pd was geplaatst, was het gemakkelijker om voor digitale sporen te kiezen.
Indien al gezocht op social media, daarna niet meer gekozen voor dit type bewijs.
Een spoor helemaal willen benutten totdat het doodloopt.
Nadat het buurtonderzoek positief was, daarna weer voor buren gekozen.
Een paar keer leverde digitaal niets op, dus daarom voor analoog gekozen.
Er zat geen enkele logica in, maar het laat je wel nadenken over de volgende keuze.
Door de vluchtigheid van gegevens vaker voor digitale sporen gekozen.
Ik had het gevoel dat digitale middelen meer info teweegbrachten.
Het positieve dan wel negatieve resultaat bepaalde de daaropvolgende stap.
Indien een vordering wordt afgewezen en/of geen iRN, dan eerder voor traditioneel gekozen om vertraging te voorkomen.
Een foto op een eerder moment, leidde tot een keuze voor de 18 GB uit de smartphone op een later moment (zodat naar die foto gezocht kon worden).
De bewijskracht lag niet in de analoge wereld.

5.2.3 *Resumé*

Er is veel verscheidenheid in keuzestrategieën en redenen die worden aangehaald om voor een bepaald bewijsstuk te kiezen. Gemiddeld genomen kiest men iets vaker voor een digitaal bewijsstuk, dan voor een analoog bewijsstuk (6,3 van de tien keer). Er wordt veelal geredeneerd vanuit de casus. Respondenten noemen bijvoorbeeld dat ze met een keuze voor een bepaald bewijsstuk inzichtelijk willen krijgen wat de contacten van de verdachte zijn of ze willen het bewijsstuk kunnen gebruiken voor het opstellen van een tijdlijn. De overweging dat een bepaald type bewijsstuk simpelweg "meer oplevert" wordt zowel voor analoge als voor digitale bewijsstukken genoemd. Dit geldt ook voor het typeren van het bewijsstuk als "betrouwbaarder" en "concreter". De redenering dat het digitale bewijsstuk "niet liegt" en een verdachte wel, komt meerdere malen terug.
Bij digitale sporen is soms de vluchtigheid ervan een reden om voor deze sporen te kiezen, en soms voeren politiemensen aan dat "dit later ook nog wel kan". Ook vonden respondenten de digitale sporen gemakkelijker om in te zetten en in te zoeken en wordt dit bewijsstuk gekozen zodat de informatie later kan worden gebruikt in een verhoor. Respondenten kozen een analoog spoor, bijvoorbeeld het verhoor of de getuigenverklaring, omdat het de mogelijkheid geeft om dóór te vragen, omdat men nieuwsgierig is naar het verhaal van een persoon en omdat het direct en snel informatie biedt. De aard van politiewerk maakt dat respondenten bij de zevende keuze kiezen voor een tweede slachtoffer dat zich meldt: "Ik vind het belangrijk dat slachtoffers te woord gestaan worden en serieus worden genomen".

Er zijn weinig significante verschillen tussen groepen in hun keuze voor een digitaal dan wel een analoog spoor. Bij één keuze kozen vrouwen duidelijk vaker voor het digitale spoor (het open bronnenonderzoek) dan mannen. Bij twee keuzes was er sprake van significante verschillen tussen leeftijdscategorieën, waarbij de leeftijdscategorie van 51 jaar en ouder in beide gevallen het vaakst koos voor het digitale spoor. Dat respondenten ervaring hebben met zaken op het gebied van digitale criminaliteit of een opleiding en/of cursus hebben gevolgd op het gebied van cybercrime/digitaal zorgt niet voor significante verschillen tussen groepen.

5.3 Politiemensen over het gebruik van digitaal bewijs

Inleiding
Deze paragraaf gaat over hoe politiemensen digitale sporen gebruiken bij opsporingsonderzoek. Bij de keuzemomenten die zijn besproken in paragraaf 5.2 is, nadat de keuze werd gemaakt, gevraagd hoe de opsporingsmedewerkers normaal gesproken met dit bewijsstuk aan de slag zouden gaan. Enkel de antwoorden bij de keuze voor het digitale bewijsstuk worden besproken. Hierna komen de tien keuzes achtereenvolgens aan bod. Steeds geven we eerst de hoofdlijn uit de bevindingen weer. Bij elke keuze staat in een box (5.1 t/m 5.10) het soort antwoorden dat de respondenten gaven. De formulering van de antwoorden is ten behoeve van de leesbaarheid hier en daar aangepast. Een box bevat niet de frequentie van de antwoorden; daarvoor zijn de respondentaantallen te laag. Een box geeft dus een indicatie van de variëteit aan handelingsstrategieën binnen de opsporing, maar toont niet waarop qua omvang de nadruk ligt. Een gedetailleerder overzicht van de toelichtingen staat in bijlage 7.

Keuze 1: Raadplegen social media. Een deel van de 44 respondenten die kozen voor het raadplegen van social media zou zelf gaan kijken op de accounts, al dan niet met behulp van een afgeschermde (iRN) computer: *"Als het niet voorhanden is, zou ik het op een normale pc doen"*. Daarnaast zouden meerdere respondenten specialisten inschakelen, bijvoorbeeld het cybercrimeteam of een internetrechercheur. Enkelen zouden de officier van justitie raadplegen over stelselmatigheid van zoeken (indien zelf wordt gezocht), dan wel over het opmaken van een vordering.

Box 5.1: Voorbeelden van handelingsstrategieën raadplegen social media

Gerichte vragen formuleren voor het opsporingsonderzoek en de telefoon afleveren bij het digitale team voor vordering en analyse.
Inloggen en screenshots maken van interessante bevindingen. Zo mogelijk met iRN.
Met hulp van de officier van justitie een vordering opmaken om de gegevens te krijgen van Instagram en Facebook.

Keuze 2: Open bronnenonderzoek. In totaal kozen 57 respondenten voor het open bronnenonderzoek (social media, fora, YouTube, etc.). Wederom is er duidelijk een splitsing tussen respondenten die zelf met het bewijsstuk aan de slag zouden gaan en

respondenten die het zouden uitbesteden, ofwel omdat ze zelf niet (volledig) over de benodigde kennis beschikken ("Ik ben digibeet") ofwel omdat ze geen tijd hebben. Een deel van de respondenten houdt rekening met eventuele juridische belemmeringen: "Je moet er wel om denken dat je niet te ver gaat". Eén respondent pakt het open bronnenonderzoek aan door een fake-account te gebruiken:

"Ik doe dit al 10 tot 15 jaar. Ik heb een fake-account opgezet en ik houd dit account levend. Ik heb een vriendengroep opgebouwd en blijf actief."

Box 5.2: Voorbeelden van handelingsstrategieën open bronnenonderzoek

Alles wat relevant is bij het zoeken op de nickname onderzoeken (wat doet hij, wat doen zijn vrienden, relaties, gesprekken, etc.).
Een collega vragen met specialistische kennis (Open Source Intelligence, iRN, digitaal rechercheur, etc.).
Zo nodig toestemming vragen van officier van justitie.

Keuze 3: Uitlezen en veiligstellen modem en router. Dit bewijsstuk is door 38 respondenten gekozen. Er is een duidelijke voorkeur voor het inschakelen van experts. Ofwel op de pd zelf, voor advies of zodat onderzoek kan worden gedaan terwijl de modem en router actief blijven, ofwel door de modem en router veilig te stellen en in te leveren bij Team Digitale Opsporing: "Ik zou daarvoor Team Digitale Opsporing benaderen. Ik kan dat zelf niet". Box 5.3 toont enkele manieren waarop respondenten normaal gesproken met dit bewijsstuk aan de slag zouden gaan.

Box 5.3: Voorbeelden van handelingsstrategieën uitlezen modem en router

Bij voorkeur ter plekke onderzoeken, zodat het verlies van gegevens wordt voorkomen.
Meenemen, veiligstellen en aan collega's van Team Digitale Opsporing overdragen.
Team Digitale Opsporing raadplegen. Zij lezen de modem/router uit en maken daar p.v. van.

Keuze 4: Geluidsopname op smartphone. Er waren 53 respondenten die kozen voor de geluidsopname op de smartphone. Bij dit bewijsstuk is er een verscheidenheid merkbaar in de werkwijzen die worden toegepast. Sommigen zouden de telefoon laten uitlezen, anderen zouden de eigenaresse van de smartphone vragen het geluidsbestand te delen. Het systeem Elvis[23] werd door meerdere respondenten genoemd als manier om digitale bestanden aan een p.v.-nummer te koppelen. Weer andere respondenten kozen voor het woordelijk uitwerken van de opname en dit toe te voegen aan het dossier middels een p.v. of voor het opvragen van het bestand middels een vordering. Ook bij dit bewijsstuk waren er respondenten die om advies zouden vragen bij digitaal experts.

23 Elvis is een softwareprogramma waarmee burgers zelf documenten/foto's/filmpjes voor de opsporing kunnen uploaden.

Tot slot wordt genoemd dat in de metadata van het geluidsbestand inzicht kan worden verkregen in de tijdlijn.

Box 5.4: Voorbeelden van handelingsstrategieën geluidsopname smartphone

Eigenaresse van de smartphone kan het bestand via e-mail of Whatsapp toesturen.
Expert bevragen over de echtheid van het geluidsbestand.
Geluidsopname innemen en het bestand woordelijk uitwerken. Het uitgewerkte bestand komt in het dossier.
Telefoon formeel in beslag nemen, naar afdeling 'digi' brengen en laten uitlezen.

Keuze 5: Monitoren Instagram. Door 55 respondenten werd gekozen voor het verzoek tot monitoren van het Instagramaccount van de verdachte. De juridische drempel van toestemming voor stelselmatige observatie werd door een groot deel van de respondenten genoemd, al zijn er enkelen die aangaven dat zij zelf iedere dag op het account zouden kijken *"Ik kijk iedere dag op het Instagram-account van [verdachte] Tony en let op nieuwe vrienden en foto's"*. Daarnaast werd genoemd dat respondenten niet weten hoe ze dit moeten aanpakken (*"Ik durf het niet te zeggen"*) en (daarom) een specialist inschakelen van binnen of buiten het team. Box 5.5 toont de genoemde handelingsstrategieën.

Box 5.5: Voorbeelden van handelingsstrategieën monitoren Instagram

Geen ervaring mee/weet niet.
Script maken, zodat veranderingen in het account worden doorgegeven (na toestemming stelselmatigheid).
Webcrawler[24] op zetten via afdeling digitaal.

Keuze 6: Inzien loggegevens app. Door 39 respondenten werd het inzien van de loggegevens van de bank-app gekozen als bewijsstuk. De werkwijze die normaal gesproken wordt gehanteerd door respondenten is gericht op het vorderen van gegevens, het inschakelen van expertise en/of het (laten) uitlezen van de telefoon. Enkele respondenten hebben geen ervaring met dit bewijsstuk: *"Ik zou hiervoor een collega raadplegen die daar meer verstand van heeft. Want het zegt mij zo niks"*. Voorbeelden van de genoemde handelingsstrategieën staan in box 5.6.

Box 5.6: Voorbeelden van handelingsstrategieën loggegevens bank-app

Laten uitlezen door afdeling digitaal.
Loggegevens gebruiken om te kijken vanaf welk IP-adres is ingelogd, met welk apparaat, naar welke rekeningen is overgemaakt, vanaf welke locatie, contante opnames van geld, etc.
Opvragen met een vordering. Toestemming van officier van justitie is nodig.

24 Een softwareprogramma dat internetpagina's doorzoekt naar bepaalde gegevens en die vastlegt.

Keuze 7: Berichten op smartphone. Er waren 47 respondenten die kozen voor de belastende berichten op de smartphone van een getuige. Respondenten kozen bij dit bewijsstuk voor het laten uitlezen van de telefoon, gegevens laten veiligstellen door Team Digitale Opsporing of de berichten door te laten appen/mailen. De meer analoge benadering kwam ook aan bod, zoals het opnemen van een getuigenverklaring of het lezen van de berichten en daar een p.v. van maken. Eén respondent noemt de factor privacy: *"Bij uitlezen krijg je álles, dan wordt de telefoon compleet gekopieerd en dan zie je alles. Als je alleen Whatsapp gebruikt is dat niet nodig en voorkom je een inbreuk op privacy"*. Box 5.7 toont enkele bij dit bewijsstuk genoemde handelingsstrategieën.

Box 5.7: Voorbeelden van handelingsstrategieën berichten op smartphone

Advies inwinnen over hoe hiermee om te gaan.
Eerst getuigenverklaring laten afleggen en dan berichten als bijlage bij p.v. toevoegen.
Indien getuige vrijwillig telefoon afstaat, kan telefoon worden ingenomen en kopie worden gemaakt.

Keuze 8: Data afkomstig uit smartphone. Zoals aangegeven in paragraaf 5.2 werd door bijna alle respondenten (74 van de 76) gekozen voor 18 GB aan data uit de uitgelezen telefoon van verdachte. Uit de antwoorden blijkt dat in de meeste gevallen de telefoon wordt uitgelezen door digitaal specialisten, waarna de rapportage kan worden doorgenomen: "*Tactisch onderzoek doen we meestal zelf"*. Sommige respondenten zeiden dat ze zelf een telefoon kunnen uitlezen: "*Als de casus zich ervoor leent dan sluit ik hem zelf aan. Met pincode heb je digitaal experts nodig. Meestal is het 1234 of 0000"*. Het filteren van informatie uit een smartphone is daarnaast van belang, al dan niet middels gerichte zoekvragen. In box 5.8 staan voorbeelden van de bij dit bewijsstuk genoemde handelingsstrategieën.

Box 5.8: Voorbeelden van handelingsstrategieën data smartphone[25]

Forensische software inzetten (bijvoorbeeld UFED of XRY[25]).
Selectief zoeken op datgene wat interessant is voor een zaak. In dit geval foto's, social media, chat en internetbankieren.
Telefoon in beslag nemen via toestemming van officier van justitie, experts lezen telefoon uit (kopie) en maken een rapportage. In de rapportage zelf zoeken naar relevante informatie.

Keuze 9: Loggegevens game. Door 27 respondenten werd gekozen voor de screenshots van de loggegevens van een game. Naar aanleiding van de aangeleverde screenshots zouden respondenten verder onderzoek doen naar de echtheid van de afbeeldingen en de vraag of het daadwerkelijk verdachte was die aan het gamen was onder de profielnaam. Daarnaast zou men digitaal experts raadplegen. Enkele respondenten zouden een p.v. opmaken: een meer analoge benadering. Ook wordt genoemd dat in overleg met officier van justitie of rechter-commissaris een vordering kan worden opgesteld bij

25 UFED (Universal Forensic Extraction Device) en XRY zijn softwareprogramma's voor (forensisch) onderzoek aan mobiele telefoons.

de game zelf. Eén respondent geeft een heldere samenvatting van een voorkeurswerkwijze:

"Ik zou gaan kijken naar de plaats, tijd en datum waarop [verdachte] aan het gamen is geweest […]. Ik zou willen onderzoeken of hij echt de gebruiker is van de profielnaam. Als ik de aangeleverde loggegevens niet snap zou ik overleggen met een digitaal specialist, anders zou ik er zelf mee aan de slag gaan denk ik. Ik zou sowieso wel met een digitaal specialist overleggen welke informatie ik er nog meer uit zou kunnen halen".

In box 5.9 staan voorbeelden van de bij dit bewijsstuk genoemde handelingsstrategieën.

Box 5.9: Voorbeelden van handelingsstrategieën screenshots game

Gegevens vorderen bij de game om te kijken of de screenshots overeenkomen met de werkelijke loggegevens.
In zorgvuldig overleg met officier van justitie over vordering tot inloggen bij de game.
Screenshots printen en bevindingen opnemen in een beeld-p.v..
Taalgebruik en overige kenmerkende eigenschappen in de game gebruiken om te controleren of het echt verdachte was.

Keuze 10: Onderzoek op dark web. Er waren 46 respondenten die kozen voor een verkenning van relevante fora op het dark web in combinatie met een nickname. Een deel van de respondenten zou dit niet zelf doen, omdat ze niet weten hoe of geen ervaring hebben: "Als het een soort Google is, dan zoek ik op die manier, maar geen idee". Hierbij wordt een verscheidenheid aan mogelijke expertises genoemd: Dienst Regionale Informatie Organisatie (DRIO), Team Digitale Opsporing (TDO), het regionale cybercrimeteam,[26] het landelijke darkwebteam, de Landelijke Eenheid (LE)[27], open-source intelligence (OSINT), Team High Tech Crime (THTC). Een respondent licht toe:

"Ik heb helemaal geen verstand van het dark web. Zou met stand alone computer moeten, maar geen idee hoe ik dat zou doen. Never nooit zou ik dat doen. Ik zou ondersteuningsdesk vragen."

Er waren echter ook respondenten die wél zelf zouden kijken op het dark web. Door met een standalone computer te gaan zoeken bijvoorbeeld. Eén respondent geeft inzichten in zijn werkwijze en zijn ervaringen met opsporingswerk op het dark web:

"Met een iRN computer die ik kan inrichten zoals ik wil. Daar zitten ook dark web browsers op. Het levert genoeg op voor politieonderzoek, maar er wordt geen moer mee gedaan. Vind ik een beetje jammer. Blank spot bij de politie. Zeker op de basisteams, daar

26 Elk van de tien regionale politie-eenheden heeft een cybercrimeteam voor cybercrimebestrijding.
27 De Landelijke Eenheid van de nationale politie verricht 'landelijke en specialistische politietaken'. (https://thesaurus.politieacademie.nl/Thesaurus/Term/9845, geraadpleegd 18 oktober 2019).

leeft het amper. Collega's hebben geen idee. Toen er aangifte werd gedaan van gebruik van vals geld vroeg men waar de drukpers stond. Vals geld bestel je gewoon op het dark web."

Box 5.10 toont voorbeelden van de bij dit bewijsstuk genoemde handelingsstrategieën.

Box 5.10: Voorbeelden van handelingsstrategieën onderzoek dark web

Een expert van de afdeling cybercrime, Dienst Regionale Informatie Organisatie, Team Digitale Opsporing of Landelijke Eenheid raadplegen en inzetten.
Geen ervaring/weet niet.
IRN computer gebruiken en zelf kijken.
THTC inschakelen.

Resumé
Uit de gegeven antwoorden op de vraag hoe respondenten normaal gesproken met digitale sporen aan de slag zouden gaan, komt naar voren dat een groot deel expertise zou inschakelen. Bijvoorbeeld bij Team Digitale Opsporing of Dienst Regionale Informatie Organisatie. Er is echter niet altijd een specifieke afdeling die wordt genoemd; "team digi' is een veelgenoemd antwoord. Kortom, respondenten geven geregeld aan dat zij bij het gebruik van digitaal bewijs een beroep op experts zouden doen, maar zijn vervolgens vaak niet zeker bij welk onderdeel ze die expertise kunnen inroepen.
Een ander deel van de respondenten is zelfredzaam en gaat, al dan niet op een standalone computer, zelf onderzoek doen naar digitale sporen. Bijvoorbeeld door naar EXIF-gegevens, IP-adressen of loggegevens te kijken. We hebben niet onderzocht of zij over de daarvoor benodigde kennis en vaardigheden beschikken.[28] Verder wordt bij diverse digitale bewijsstukken door respondenten voor een analoge verwerking gekozen. Bij een geluidsopname van de smartphone waren bijvoorbeeld respondenten die de opname zouden afluisteren en woordelijk zouden opnemen in een proces-verbaal.
Tot slot noemen respondenten handelingsstrategieën die gericht zijn op de juridische aandachtspunten om digitaal sporenonderzoek verder op te pakken. Bijvoorbeeld door een vordering in te dienen bij Facebook of toestemming te vragen voor het uitlezen van een smartphone.

5.4 Algemene ervaringen met gebruik digitale sporen

Inleiding
De laatste paragraaf van dit hoofdstuk gaat over de antwoorden op een afsluitende vraag in het casusonderzoek: 'Wilt u verder nog iets toelichten over uw ervaringen met het gebruik van digitale sporen?'. Deze vraag is door respondenten op verschillende

28 Het onderzoek van Van Valkengoed (2017) naar digitale kennis en vaardigheden van rechercheurs in Amsterdam laat zien dat die over het geheel genomen te wensen over laten, maar het is natuurlijk mogelijk dat de respondenten die aangeven dat zij zelf met digitale sporen zouden gaan werken, juist wél over de daarvoor benodigde kennis en vaardigheden beschikken. Zie ook bijlage 10.

manieren geïnterpreteerd en beantwoord. Het gros heeft een antwoord gegeven dat ingaat op persoonlijke ervaringen met digitale sporen (N=52). Daarom zijn de gegeven antwoorden die hierop gericht waren eerst geclusterd in hoeveelheid ervaring (weinig, enigszins, veel) (zie paragraaf 5.4.1). Deze indeling is enkel gemaakt op basis van de inhoud van de antwoorden op de zojuist genoemde open vraag.
Daarnaast waren antwoorden (deels) gericht op het gebruik van digitale sporen bij de politie in het algemeen. Ten derde kwam bij een deel van de respondenten de mogelijkheden, waarde en beperkingen van digitale sporen aan bod. Tot slot werd door sommige respondenten een vergelijking gemaakt tussen digitale en analoge sporen (zie paragraaf 5.4.2).
Ten behoeve van de leesbaarheid is een selectie gemaakt in het aantal toelichtingen bij ieder deelthema. Er is gekozen voor citaten die kenmerkend zijn voor de antwoorden die gegeven zijn. In bijlage 8 zijn alle toelichtingen opgenomen.

5.4.1 *Ervaringen met digitale sporen op basis van hoeveelheid ervaring*

Weinig ervaring. Uit de gegeven antwoorden blijkt dat de respondenten die (heel) weinig ervaring hebben met het gebruik van digitale sporen, wel digitale sporen tegenkomen in hun werk en ook inzien dat het in de toekomst steeds meer zal voorkomen. Verder gaven deze respondenten aan dat ze weten waar ze de benodigde digitale expertise vandaan kunnen halen indien ze tijdens hun werkzaamheden worden geconfronteerd met digitale sporen. Hoewel hetzelfde beeld naar voren kwam in paragraaf 5.3 (bij de keuze voor een digitaal bewijsstuk werd regelmatig aangegeven dat een expert zou worden geraadpleegd bij het gebruik ervan), werd daarin wel duidelijk dat respondenten niet precies weten welke expert ze bij welke vraag aan de jas moeten trekken. Dit strookt derhalve niet met elkaar. Dat kan komen door verschillen in vraagstelling en/of het feit dat deze groep weinig ervaring heeft met digitale sporen. Een andere verklaring is dat als politiemedewerkers heel concreet moeten worden, ze het moeilijk vinden te benoemen bij wie ze precies moeten zijn. Dit is echter niet verder onderzocht.
Er zijn veel respondenten binnen deze groep die proberen met digitale sporen aan de slag te gaan, bijvoorbeeld via open bronnenonderzoek en het (laten) uitlezen van een telefoon. Een enkeling heeft cursussen gevolgd, maar de daarbij opgedane kennis is weggezakt. Box 5.11 geeft een overzicht van de antwoorden van de 22 respondenten met weinig ervaring met digitale sporen.

Box 5.11: Weinig ervaring met digitale sporen

Ik heb weleens een telefoon laten uitlezen en bankgegevens, verder dan dat ben ik nog niet gekomen. Met de telefoon heeft wel echt de toekomst, als je kijkt naar jeugd is de telefoon hun leven.
Omdat ik er minder ervaring mee heb, stel ik de vraag altijd wel aan digi, waarbij ik de casus voorleg, en vraag of er nog digitale mogelijkheden zijn.
Wat ik vervelend vind voor mijzelf is dat het best wel weg is gezakt. Ik merk dat ik soms zoiets heb van hoe ging dat ook alweer.

Enigszins ervaring. In box 5.12 staan enkele citaten van de 22 respondenten die enigszins ervaring hebben met digitale sporen. Zij gaven aan digitale sporen te gebruiken omdat ze eerder al successen hebben behaald met onder andere bankgegevens, het uitlezen van telefoons en social media. Diverse respondenten refereerden aan een "digitale mindset", waarbij zo nodig expertise wordt opgezocht. Eén respondent verwoordde het als volgt: *"Ik vind het belangrijk om te kunnen signaleren en om te kunnen weten waar de kansen liggen om een specialist daarover te bevragen"*.

Box 5.12: Enigszins ervaring met digitale sporen

Ik ben bij ons wel degene die veel met digitale sporen en cybercrime doet. Ik denk dat het soms ook wel is van in het land der blinden. Ik gebruik wel social media om ernaar te kijken voordat ik iemand uitnodig voor verhoor. Het dark web check ik ook wel eens.
Ik werk nu een jaar bij het cybercrimeteam en ik leer elke dag. Er is een hele wereld voor me opengegaan. Ik ben nog steeds een digibeet. Ik ben heel blij met hoe ver ik ben. Niveau is absoluut gegroeid. Nu maak ik tapaanvragen en doe ik van alles.
Mijn mindset gaat richting digitaal, maar ik laat het rechercheren over aan deskundigen, omdat ik een onderzoek niet wil verknoeien.

Veel ervaring. In box 5.13 staan de antwoorden van de respondenten die veel ervaring hebben met digitale sporen. Deze ervaren respondenten gaven aan dat ze in korte tijd resultaten kunnen boeken. Werkzaamheden bestaan bijvoorbeeld uit het (laten) uitlezen van telefoons en computers en uit open bronnenonderzoek.

Box 5.13: Veel ervaring met digitale sporen

Daar werk ik bijna dagelijks mee. Ik doe alle tactische werkzaamheden. Ik bekijk veel uitgelezen telefoons. Veel tappen, verhoren. Open bronnenonderzoek.
Ik gebruik een iRN op de werkplek. Zeker bij evenementen kijken we wat er speelt. Ook wel bij specifieke zaken en dan komen ze bij mij om te zoeken. […] We gebruiken ook digitaal om mensen te bereiken en over zaken te informeren.
Ik gebruik het in mijn werk heel veel eigenlijk. Mijn crimeteam heeft geen kennis/kunde, dus dan vragen ze mij.

5.4.2 *Overige opmerkingen over het gebruik van digitale sporten bij de politie*

Deelnemers uitten ook meer algemene opmerkingen over het gebruik van digitale sporen binnen het politieapparaat (zie box 5.14). Ten eerste werd gesproken over het ge-

brek aan kennis op de werkvloer, met name over de mogelijkheden die digitale sporen kunnen bieden. Hoewel meerdere respondenten noemden dat ze zelf met digitale sporen aan de slag gaan, werd ook aangegeven dat men bijvoorbeeld wel zelf een telefoon wil uitlezen, maar dat dat niet mag. Of dat er angst is om fouten te maken. Eén respondent spreekt over een *"hele grote hang naar de traditionele kant"*. Een andere respondent zei: *"We lopen hopeloos achter"*.

Sommige respondenten gaven aanbevelingen voor de toekomst: het digitaal bewust maken van iedereen in de politieorganisatie, duidelijkheid over welk team welke zaak oppakt, de internettap beter benutten, meer tijd en capaciteit voor het (beter) gebruiken van digitale sporen, betere beschikbaarheid van digitale expertise, meer gebruikmaken van digitale kennis bij het verhoor en dat wat geleerd is tijdens de cursus blijven oefenen. Eén respondent merkte op: *"Op straat worden de kansen nog niet altijd gezien"*. Tot slot ging een respondent in op de privacy van verdachten. Men gaat bijvoorbeeld 'even kijken" achter de eigen werkplek op social media-kanalen, terwijl dit potentieel zeer nadelig kan zijn en in strijd met de wetgeving, in het bijzonder art. 8 EVRM.

Box 5.14: Over het gebruik van digitale sporen bij de politie

Er is veel te halen, maar de kennis is beperkt. Vaak wordt iemand erbij gehaald die kennis heeft. Mensen willen geen fouten maken als ze het zelf doen.
Ik heb een iRN cursus gedaan. Dat duurde toen nog twee jaar voordat we zo'n computer kregen, dus toen wist ik niet meer hoe ik het geleerde moest toepassen. […] Heel jammer dat ik kennis kwijt ben.
Ik vind dat mensen er te weinig vanaf weten en dat het als een soort exotisch iets wordt beschouwd. Tegelijkertijd doen de mensen die er meer vanaf weten er nogal eens te 'spastisch' over.
Per basisteam zouden we één iemand van het crimeteam moeten aanwijzen die zich mag verdiepen in digitale zaken. Ik krijg wel de ruimte daarvoor, maar wij zijn het enige team denk ik.

Mogelijkheden, waarde en beperkingen van digitale sporen
Qua mogelijkheden werd aangegeven dat digitale sporen heel veel kunnen opleveren: *"Er is zo absurd veel dat je kunt vinden"*. Live chatcontact achten respondenten een belangrijke bron van informatie, net als het landelijk delen van digitale informatie.

In het algemeen werd gesproken over de toekomstbestendigheid en bewijswaarde van digitale sporen. Digitale sporen *"liegen niet"*. Bovendien kan informatie uit digitale bronnen worden gebruikt voor het verhoor.

Beperkingen werden gezien in de tijd die het kost om tot relevante resultaten te komen. Het is niet altijd *"doorslaggevend"*. Daarnaast zijn digitale sporen vluchtige gegevens die snel weg zijn en gemanipuleerd kunnen worden. Een respondent noemde dat het moeilijk is om een analoog persoon aan een digitale identiteit te koppelen.

Box 5.15: De waarde, mogelijkheden en beperkingen van digitale sporen

Digitale sporen kunnen snel weg zijn en gemanipuleerd worden. Moeilijk om grip op te krijgen. Moeilijk om analoog persoon aan digitale identiteit te koppelen.
Je weet soms niet op welk moment je het wel/niet kunt gebruiken. Bij zeden ben je vaak te laat. Er gaat vaak tijd overheen en je start meestal met een getuige. Gegevens zijn dan soms al verloren gegaan.
Mooie resultaten mee gehaald in onderzoeken. In een zaak verklaarde verdachte dat hij zich op plaats X bevond, maar wij konden digitaal aantonen dat het plaats Y was. De rechter vond zijn verklaring vervolgens leugenachtig op dat punt. Positieve ervaring dus.

Digitaal vs. analoog

Tot slot blijkt uit enkele antwoorden dat het gebruik van digitale sporen als lastiger wordt ervaren met meer juridische drempels, maar dat het ook meer kan opleveren dan klassieke opsporingsmethoden. Niet iedere politiemedewerker denkt aan de digitale mogelijkheden bij het zoeken naar informatie: *"Alsof we vroeger bijvoorbeeld overal zochten naar een telefoonnummer, behalve in het telefoonboek"*.

Box 5.16: Digitale sporen versus analoge sporen

Het is lastiger. Je moet een vordering hebben, dingen regelen. Al het fysiek aanwezige kun je op papier zetten. Daar heb je geen officier van justitie voor nodig, gaat sneller.
Op basis van telefoongegevens kun je al wel goed vaststellen hoe iemand beweegt. Uit telefoons haal je best veel informatie. Het is dus belangrijk om hier goed naar te kijken, vooral ook omdat de technische sporen, zoals DNA, er vaak niet zijn zodat je op andere wegen bent aangewezen, ook omdat er nogal eens geen getuigen zijn.

Resumé

Uit de antwoorden van de respondenten over hun ervaringen met digitale sporen blijkt dat veel respondenten de mogelijkheden van digitale sporen inzien. De politie kan niet meer om digitale sporen heen en diverse respondenten noemen de nuttige en vele mogelijkheden die digitale sporen kunnen bieden. Dat er nog stappen gezet moeten worden binnen de politie wordt ook erkend. De expertise op het gebied van digitaal groeit, maar de digitale mindset zou bij alle politiemensen aanwezig moeten zijn. Een kleinere groep respondenten is zelf dagelijks aan de slag met digitale sporen. Een groter deel heeft weinig ervaring. Zij geven echter ook aan dat ze veel met digitale sporen te maken hebben, maar daarvoor (nu nog) expertise moeten inschakelen. Dat er ontwikkelingen gaande zijn blijkt met name uit de groep met redelijk veel ervaring: men geeft aan steeds meer te leren over de mogelijkheden van digitale sporen en kansen steeds beter te benutten. In de waardering van digitale sporen zien we een tegenstrijdigheid: politiemensen zeggen "digitale sporen liegen niet", terwijl we tegelijk van hen horen dat dergelijke sporen "gemanipuleerd kunnen worden".

6. Intentie tot het gebruik van digitale sporen

6.1 Inleiding

In dit hoofdstuk wordt de volgende deelvraag beantwoord: 'In hoeverre hebben politiemensen de intentie om digitale sporen te gebruiken bij opsporingsonderzoek en in hoeverre handelen ze naar hun intenties?' Nadat is ingegaan op de intenties tot het gebruik van digitale sporen, wordt de relatie besproken tussen intenties en daadwerkelijk gedrag.

6.2 Intentie tot gebruik van digitale sporen

Uit diverse wetenschappelijke studies blijkt dat intenties voor een belangrijk deel gedrag kunnen verklaren. Dit komt voort uit de Reasoned Action Approach (RAA) van Fishbein en Ajzen (2010). De RAA stelt kortgezegd dat intentie tot gedrag de beste voorspeller is voor daadwerkelijk gedrag. Wanneer er daarom inzicht is in de intenties van politiemensen om digitale sporen te gebruiken, kunnen we waarschijnlijk ook iets zeggen over of zij daadwerkelijk digitale sporen (zullen) gebruiken.
In de vragenlijst zijn drie stellingen voorgelegd aan de 75 respondenten[29] over hun intentie om digitale sporen te gebruiken (zie bijlage 6). De formulering van deze stellingen sluit aan bij de RAA van Fishbein en Ajzen (2010). De stellingen waren als volgt:

1. Ik heb de intentie om de komende maand digitale sporen te gebruiken om aan een zaak te werken.
2. Ik ben van plan de komende maand digitale sporen te gebruiken om aan een zaak te werken.
3. Ik verwacht dat ik de komende maand digitale sporen ga gebruiken om aan een zaak te werken.

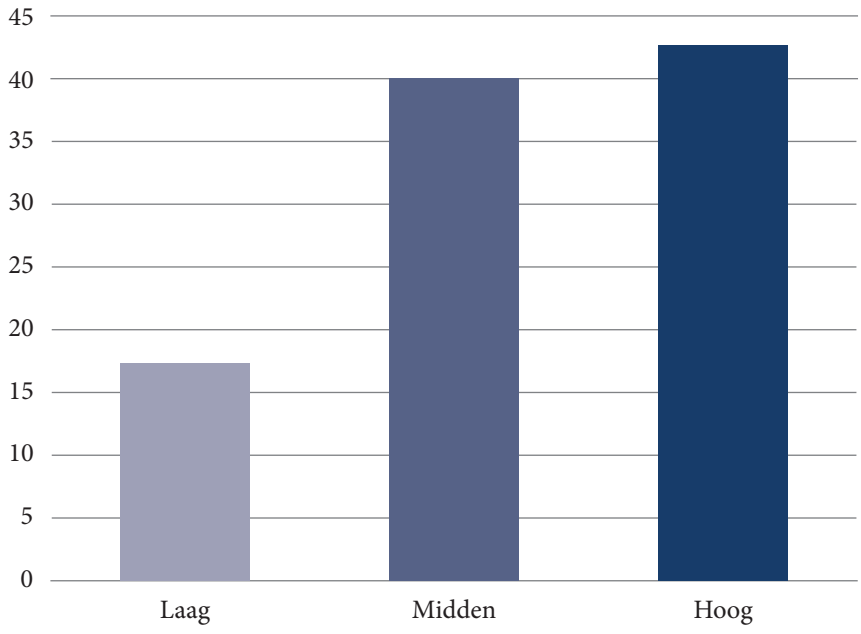
Op alle drie de stellingen kon geantwoord worden op een zevenpunts Likertschaal van 'helemaal mee oneens' tot 'helemaal mee eens'. De betrouwbaarheid van de schaal is α=.9.

29 Eén respondent heeft deze vragen niet ingevuld.

Intentie om digitale sporen te gebruiken
De maximale score op de intentieschaal is 7. Gemiddeld is er 5,1 gescoord, met een standaarddeviatie van 1,7.

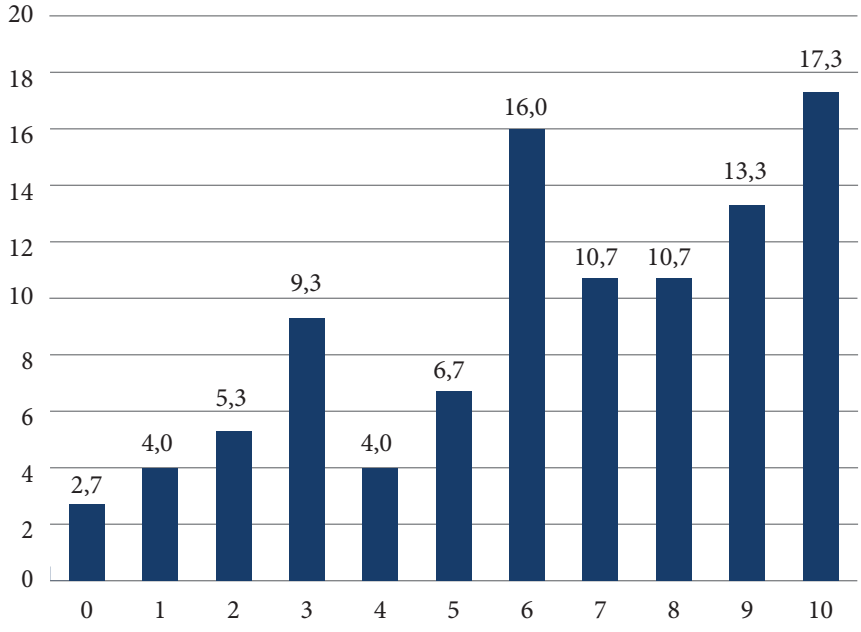
In grafiek 6.1 zijn de resultaten visueel weergeven. De scores zijn verdeeld in (gemiddeld) een lage score (1-3), een midden score (4-5) of een hoge score (6-7). Twee op de vijf respondenten scoort midden (40%) en 42,7 procent van de respondenten scoort hoog op de intentie voor het gebruiken van digitale sporen.

Grafiek 6.1: Intenties om (de komende maand) digitale sporen te gebruiken (N=75, in procenten)



Daarnaast is een controlevraag gesteld over de intentie om digitale sporen te gebruiken. Die vraag is als volgt geformuleerd: 'Stel dat u de komende maand aan tien zaken werkt. In hoeveel van die zaken verwacht u gebruik te maken van digitale sporen?'. Het gemiddeld gegeven antwoord was 6,4 met een standaarddeviatie van 2,9. Dertien respondenten hebben aangegeven in (alle) tien zaken digitale sporen te zullen gebruiken. Dit is tevens het meest gegeven antwoord (modus). In grafiek 6.2 zijn de resultaten visueel weergegeven.

Grafiek 6.2: In hoeveel van de tien zaken verwachten respondenten de komende maand digitale sporen te gebruiken? (N=75, in procenten)



Herhaalvragenlijst. De stellingen over intenties zijn enkele weken na het casusonderzoek opnieuw bevraagd bij de respondenten.[30] Dit is gedaan om te controleren op mogelijke beïnvloeding door het net afgenomen casusonderzoek. Deze vragenlijst is door 54 respondenten ingevuld (tabel 6.1). De gemiddelde score op intentie was in de herhaalvragenlijst 5,5[31] met een standaarddeviatie van 1,4.

Tabel 6.1: Gegeven antwoorden op de intentie-stellingen in de herhaalvragenlijst (N=54, in procenten)

	Helemaal mee oneens (1)	2	3	4	5	6	Helemaal mee eens (7)
Stelling 1	0	1,3	2,6	9,2	11,8	23,7	22,4
Stelling 2	0	5,3	1,3	11,8	10,5	18,4	23,7
Stelling 3	1,3	6,6	5,3	5,3	11,8	18,4	22,4

30 Ditmaal was de Cronbach's alpha .93.
31 Iets hoger dan vlak na het casusonderzoek (5,1 met N=75).

Ook is in de herhaalvragenlijst de controlevraag gesteld over de intentie om digitale sporen te gebruiken: 'Stel dat u de komende maand aan tien zaken werkt. In hoeveel van die zaken verwacht u gebruik te maken van digitale sporen?' Het gemiddeld gegeven antwoord was 6,3 met een standaarddeviatie van 2,8. Dit is vergelijkbaar met de resultaten uit de eerste vragenlijst (6,2 zaken).

Resumé
Het gros van de respondenten heeft de intentie om digitale sporen te gebruiken. Wanneer zij een voorspelling maken van het gebruik van digitale sporen in tien zaken in de komende maand, verwachten zij in bijna twee derde van de zaken gebruik te maken van digitale sporen.

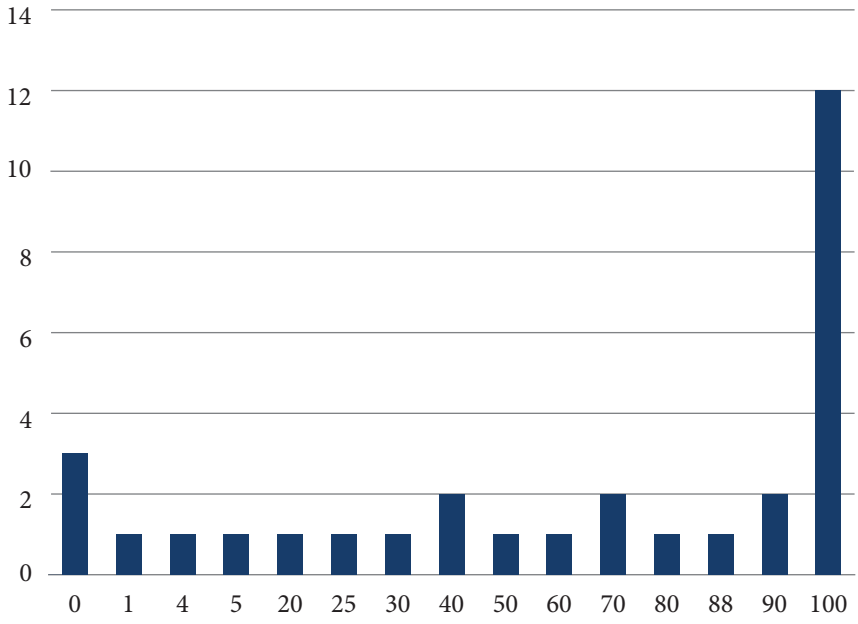
6.3 Verband tussen intenties en gedrag

Vervolgens wordt ingegaan op de vraag in hoeverre politiemensen handelen naar hun intenties om digitale sporen te gebruiken. Om deze vraag te kunnen beantwoorden, wordt eerst inzicht verkregen in het handelen van de respondenten: het daadwerkelijke gebruik van digitale sporen.

Aan respondenten is een maand na deelname aan het casusonderzoek de volgende vraag gesteld: 'In hoeveel procent van de zaken die je de afgelopen maand hebt gedraaid, heb je gebruikgemaakt van digitale sporen?' Deze vraag is beantwoord door 31 respondenten.[32] Het gemiddelde percentage betreft 62,1 procent van de zaken met een standaarddeviatie van 39,7 procent. Er is derhalve veel spreiding in het gegeven antwoord. Er zijn zes respondenten die in 0 tot 5 procent van de zaken digitale sporen hebben gebruikt en twaalf respondenten die in alle zaken digitale sporen hebben gebruikt. Grafiek 6.3 geeft de spreiding van antwoorden visueel weer.

32 Het kan zijn dat deze groep afwijkt van de 76 respondenten die hebben deelgenomen aan het casusonderzoek. We hebben dit echter niet met onderzoek kunnen vaststellen.

Grafiek 6.3: In hoeveel procent van de zaken in de afgelopen maand is gebruikgemaakt van digitale sporen? (N=31, in aantallen)



Verband tussen intenties en gedrag

Vervolgens is het verband getoetst tussen intentie en gedrag (N=31), zodat kan worden onderzocht of politiemensen handelen naar hun intenties om digitale sporen te gebruiken. Gedrag is gemeten met eerdergenoemde vraag: 'In hoeveel procent van de zaken is in een maand tijd gebruikgemaakt van digitale sporen?' Uit de correlatietoets blijkt dat er geen significant verband is tussen intentie en gedrag (r=.329, p=.076).

In een onderzoek bij zzp'ers en mkb-bedrijven zagen we ook dat men bij digitaal/cybercrime niet altijd handelt naar intenties (Veenstra, Zuurveen & Stol, 2015). In dat onderzoek kwam naar voren dat meer dan 60 procent van de respondenten zei aangifte te zullen doen van cybercrime indien zij slachtoffer zouden worden, maar slechts 7,2 procent van de mkb-bedrijven en 13 procent van de zzp'ers deed daadwerkelijk aangifte na slachtofferschap.

Factoren die correleren met intentie en gedrag

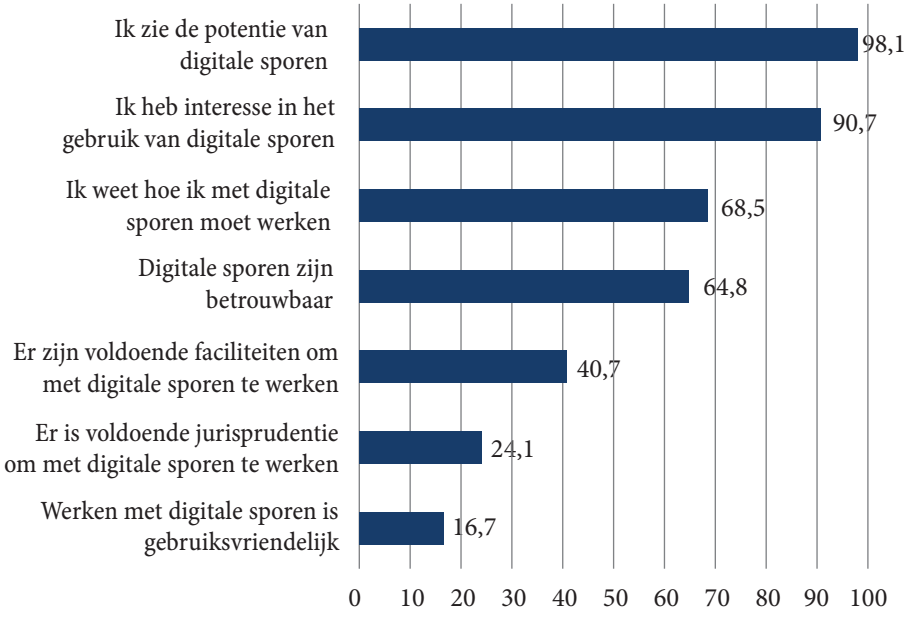
Aansluitend is onderzocht welke factoren mogelijk kunnen verklaren waarom politiemensen de intentie hebben om digitale sporen te gebruiken dan wel waarom politiemensen digitale sporen daadwerkelijk gebruiken. Daartoe wordt eerst inzicht gegeven in hoeverre respondenten bepaalde factoren herkennen.

De factoren die aan de respondenten zijn voorgelegd, zijn geformuleerd op basis van hoofdstuk 4 ('Factoren die het gebruik van digitale sporen belemmeren') en in de vragenlijst bevraagd door middel van stellingen (zie tabel 6.2). De factoren zijn zodanig geformuleerd dat in de helft van de gevallen de formulering positief is en in de helft van de gevallen negatief. Grafiek 6.4 en 6.5 geven een visuele weergave van het deel van de respondenten dat een stelling met 'enigszins mee eens' of 'helemaal mee eens' heeft beantwoord (zie bijlage 9 voor een volledig overzicht).

Tabel 6.2: Stellingen op basis van hoofdstuk 4

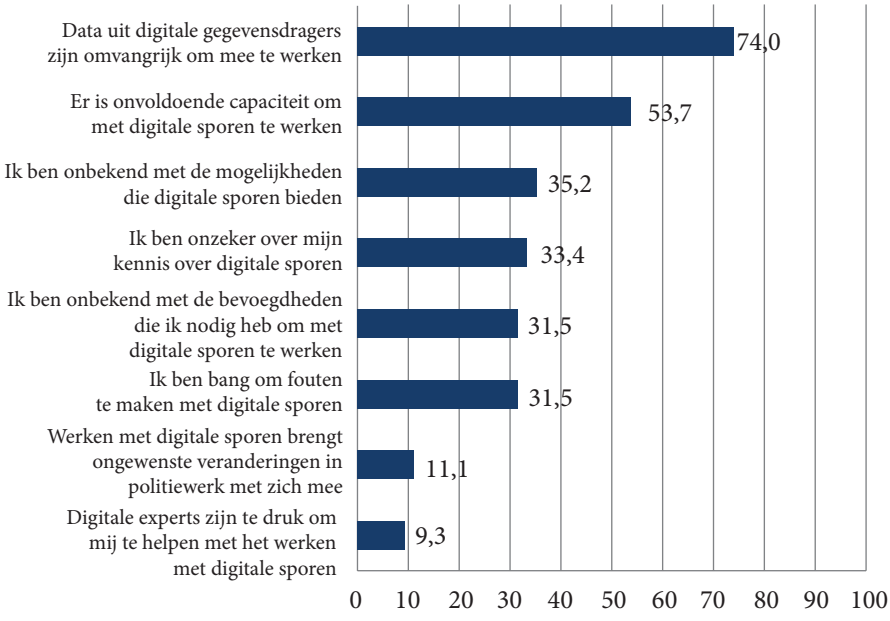
Ik weet hoe ik met digitale sporen moet werken
Ik ben onbekend met de mogelijkheden die digitale sporen bieden
Ik zie de potentie van digitale sporen
Er zijn voldoende faciliteiten om met digitale sporen te werken
Ik ben bang om fouten te maken met digitale sporen
Werken met digitale sporen is gebruiksvriendelijk
Digitale experts zijn te druk om mij te helpen met het werken met digitale sporen
Ik ben onbekend met de bevoegdheden die ik nodig hem om met digitale sporen te werken
Er is voldoende jurisprudentie om met digitale sporen te werken
Data uit digitale gegevensdragers zijn omvangrijk om mee te werken
Er is onvoldoende capaciteit om met digitale sporen te werken
Digitale sporen zijn betrouwbaar
Ik heb interesse in het gebruik van digitale sporen
Ik ben onzeker over mijn kennis over digitale sporen
Werken met digitale sporen brengt ongewenste veranderingen in politiewerk met zich mee

Grafiek 6.4: Percentage respondenten dat het enigszins of helemaal eens is met de stelling – positieve stellingen (N=54)



Uit de antwoorden op de stellingen komt naar voren dat vrijwel alle respondenten de potentie zien van digitale sporen (98,1% enigszins/helemaal mee eens). Dit is ook terug te zien bij de interesse in het gebruik van digitale sporen. Meer dan 90 procent is het enigszins of helemaal eens met deze stelling (90,7%). Daarnaast is het gros het enigszins of helemaal eens met de stelling 'Ik weet hoe ik met digitale sporen moet werken' (68,5%) en vindt bijna twee derde digitale sporen betrouwbaar (64,8%). In mindere mate wordt de beschikbaarheid van faciliteiten en jurisprudentie om met digitale sporen te werken positief beoordeeld (40,7 en 24,1%). Slechts 16,7 procent vindt werken met digitale sporen gebruiksvriendelijk.

Grafiek 6.5: Percentage respondenten dat het enigszins of helemaal eens is met de stelling – negatieve stellingen (N=54)



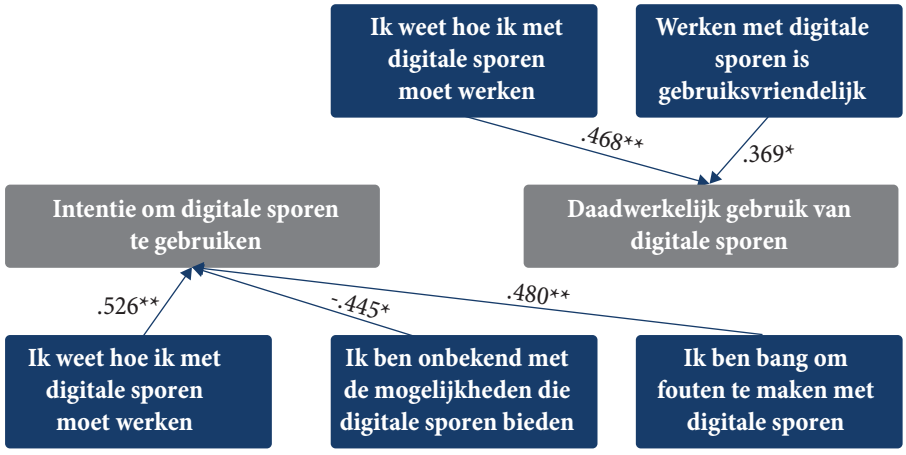
De antwoorden op de stellingen laten zien dat bijna driekwart van de respondenten data uit digitale gegevensdragers omvangrijk vindt om mee te werken (74,0%).[33] Iets meer dan de helft is het eens met de stelling dat er onvoldoende capaciteit is om met digitale sporen te werken (53,7%). Ongeveer een derde van de respondenten geeft aan dat er sprake is van onbekendheid met de mogelijkheden van digitale sporen en de benodigde bevoegdheden bij het gebruik ervan (35,3 en 31,5%). Ook is ongeveer een derde onzeker over zijn of haar kennis over digitale sporen en/of bang om fouten te maken met digitale sporen (33,4 en 31,5%). Een klein deel is het eens met de stelling dat werken met digitale sporen ongewenste veranderingen met zich meebrengt dan wel dat digitale experts te druk zijn om te helpen bij het werken met digitale sporen (11,1 en 9,3%).

Vervolgens is door middel van correlatietoetsen onderzocht wat het verband is tussen de antwoorden op de stellingen en de intentie om digitale sporen te gebruiken dan wel het daadwerkelijke gebruik ervan. Deze analyse is gedaan op basis van de antwoorden van 31 respondenten. Dat is een kleine en wellicht selectieve groep, waardoor we geen

33 Dat is niet per se negatief: politiemensen kunnen het ook een voordeel vinden dat er veel data is om mee te werken.

directe conclusies kunnen verbinden aan de resultaten. Het geeft wel een verkennend beeld. In bijlage 11 staat een volledig overzicht van alle correlaties. In figuur 6.1 zijn alleen de significante verbanden weergegeven.

Figuur 6.1: Significante verbanden (N=31)



Er is een middelmatig, significant verband tussen de antwoorden op de stelling 'Ik weet hoe ik met digitale sporen moet werken' en de intentie om digitale sporen te gebruiken. Dit betekent dat hoe beter respondenten inschatten dat ze met digitale sporen kunnen werken, hoe hoger de intentie tot het gebruik van digitale sporen (*r*=.526, *p<.01)*.
Daarnaast zijn er significante, negatieve correlaties tussen de antwoorden op de stellingen 'Ik ben onbekend met de mogelijkheden die digitale sporen bieden' en 'Ik ben bang om fouten te maken met digitale sporen' en de intentie om digitale sporen te gebruiken (respectievelijk *r*=-.445, *p*<.05 en *r*=-.480, *p*<.01). Dit wil zeggen dat indien er minder sprake is van onbekendheid met de mogelijkheden en minder angst voor het maken van fouten, de intentie tot het gebruik van digitale sporen hoger is. Hoewel deze correlaties significant zijn, is het niet een sterk verband (kleiner dan .5).

Net als voor intentie, is er een significant verband tussen de antwoorden op de stelling 'Ik weet hoe ik met digitale sporen moet werken' en het daadwerkelijke gebruik van digitale sporen. Respondenten gebruiken vaker digitale sporen wanneer ze inschatten dat ze weten hoe ze met digitale sporen moeten werken (*r*=.468, *p<.01)*. Het is echter een redelijk zwak verband.
Ten tweede blijkt uit de resultaten dat indien respondenten vinden dat het werken met digitale sporen gebruiksvriendelijk is, zij vaker digitale sporen gebruiken (*r*=.369, *p<.05*). Ook dit verband is zwak (kleiner dan .4).

Resumé
In deze paragraaf is ingegaan op de intentie van politiemensen om digitale sporen te gebruiken en in hoeverre ze handelen naar hun intenties (door digitale sporen daadwerkelijk te gebruiken). Gemiddeld gebruiken de respondenten in bijna twee derde van de zaken digitale sporen. De spreiding in antwoorden is echter groot. Uit de resultaten blijkt dat er geen verband is tussen intentie en dit gebruik. In tegenstelling tot de RAA kunnen we daarom niet concluderen dat intentie tot het gebruik van digitale sporen verband houdt met het daadwerkelijke gebruik ervan.
Er zijn significante, (redelijk) zwakke verbanden gevonden tussen intentie tot het gebruik van digitale sporen en minder angst voor het maken van fouten dan wel minder onbekendheid met de mogelijkheden van digitale sporen. Ook is er meer intentie tot gebruik wanneer respondenten inschatten dat ze met digitale sporen kunnen werken.
Het daadwerkelijke gebruik van digitale sporen is hoger wanneer respondenten denken dat ze weten hoe ze met digitale sporen moeten werken. Het is echter een redelijk klein verband. Ook is er een klein, significant verband tussen daadwerkelijk gebruik en gebruik indien respondenten vinden dat het werken met digitale sporen gebruiksvriendelijk is.
In geheel paragraaf 6.3 wordt een verkennend beeld gegeven. Omdat de respondentaantallen klein zijn, kunnen we geen directe conclusies verbinden aan de resultaten.

6.4 Factoren die het verband tussen intentie en gedrag mogelijk beïnvloeden

Als laatste is onderzocht of het verband tussen intentie en gedrag wordt beïnvloed door de factoren uit de vorige paragraaf (zie tabel 6.2). Dit is gedaan door de partiële correlaties te analyseren, waarbij de correlatie tussen intentie en gedrag is vastgesteld, gecorrigeerd voor iedere factor. Hier zijn echter geen significante resultaten uit naar voren gekomen. De volledige tabel met partiële correlaties is opgenomen in bijlage 11.

Resumé
In deze paragraaf is onderzocht door welke factoren een eventuele discrepantie tussen de intentie om digitale sporen te gebruiken en het daadwerkelijke gebruik ervan kan worden verklaard. Hieruit komt naar voren dat de mogelijkheden en belemmeringen die digitale sporen kunnen bieden, niet het gevonden (zwakke) verband tussen de intentie tot het gebruik van digitale sporen en het daadwerkelijke gebruik ervan beïnvloeden.

Noot
In bijlage 12 is een aanvullende analyse uitgevoerd waarin de volgende vraag is beantwoord: in hoeverre zijn er verschillen met betrekking tot de intentie tot en het gebruik van digitale sporen tussen respondenten die een cursus met betrekking tot digitale criminaliteit hebben gevolgd en respondenten die geen cursussen hebben gevolgd? Onder andere omdat in deze analyse gedrag (het daadwerkelijke gebruik van digitale sporen) op een andere manier is gemeten dan in onderhavig onderzoek, is het niet opgenomen in de lopende tekst van dit rapport.

7. Conclusies en slotoverwegingen

In dit hoofdstuk worden de conclusies achtereenvolgens besproken van de drie onderzoeksvragen die centraal stonden:

1. Welke niet-technische factoren belemmeren het tactisch gebruik van digitale sporen door politiemensen?
2. In hoeverre en op welke wijze gebruiken politiemensen digitale sporen bij opsporingsonderzoek?
3. In hoeverre hebben politiemensen de intentie om digitale sporen te gebruiken bij opsporingsonderzoek en in hoeverre handelen ze naar hun intenties?

Het hoofdstuk sluit af met overkoepelende bevindingen van de gehele rapportage. Ook worden er overwegingen gegeven voor toekomstig politiebeleid.

7.1 Knelpunten en mogelijkheden: resultaten uit literatuur en interviews

In deze paragraaf beantwoorden we de eerste onderzoeksvraag: 'Welke niet-technische factoren belemmeren het tactisch gebruik van digitale sporen door politiemensen? ' Dit valt uiteen in verschillende thema's.

Het eerste thema betreft beperkte kennis. Uit de literatuur blijkt dat politiemedewerkers zonder digitale expertise onvoldoende kennis hebben over bijvoorbeeld het uitlezen van gegevensdragers en de internettap en dat er te weinig inzicht is in digitale mogelijkheden. Dit leidt ertoe dat men bijvoorbeeld niet de goede vragen kan stellen in het opsporingsonderzoek. Het volgen van cursussen en opleidingen kan ervoor zorgen dat de benodigde kennis wordt opgedaan. Dit vraagt echter tevens om een investering in het laten beklijven van opgedane kennis, bijvoorbeeld door te blijven oefenen. Dat wordt lang niet altijd gedaan.
In de interviews wordt dit beeld deels bevestigd. Er zijn bijvoorbeeld nog veel vragen en onduidelijkheden bij het gebruik van digitale sporen. Experts plaatsen hun vraagtekens bij de effectiviteit van bestaande opleidingen op digitaal gebied. Er wordt echter ook aangegeven dat er positieve ontwikkelingen gaande zijn en er steeds meer aandacht is voor het gebruik van digitale sporen.
In hoofdstuk 5 kwam naar voren dat politiemensen veelal kiezen voor digitale sporen en vervolgens te rade gaan bij experts voor hulp. Dat lijkt een goede werkwijze, waarbij een gebrek aan kennis een minder groot bezwaar is.

Het tweede thema gaat over praktische factoren. Uit de literatuur blijkt dat een gebrek aan faciliteiten en personeel een probleem is, bijvoorbeeld doordat er geen iRN-computers beschikbaar zijn. Intranet biedt versnipperde informatie en digitaal experts hebben te weinig tijd om vragen van collega's te beantwoorden. Digitale sporen zijn vluchtig en daardoor snel verdwenen. Door het internationale karakter treden vertraging en taalbarrières op.
In tegenstelling tot de literatuur, komt uit de interviews naar voren dat de beperkte beschikbaarheid van faciliteiten geen belemmering (meer) vormt. Digitaal experts zijn daarnaast toegankelijker doordat ze niet meer op een aparte afdeling worden geplaatst, maar midden in de teams die opsporingswerk verrichten. In hoeverre deze bevindingen kunnen worden gegeneraliseerd naar het hele land, is de vraag. Onze respondenten kwamen voornamelijk uit de Eenheid Noord-Nederland (56 van de 76). Wel ervaart men verouderde, versnipperde informatie op intranet en een gebrek aan capaciteit. Ook wordt de grote hoeveelheid data uit gegevensdragers als knelpunt ervaren: het kost veel tijd om digitale sporen goed te onderzoeken.

Het derde thema betreft juridische knelpunten. Art. 3 PolW biedt ruimte, maar slechts voor een geringe inbreuk op de grondrechten. Het smartphone-arrest leidde ertoe dat devices niet zomaar volledig mogen worden uitgelezen, omdat ze zeer veel persoonlijke informatie bevatten. Ook het (stelselmatig) zoeken in openbare bronnen wordt juridisch beperkt. Doordat digitale sporen zich niet aan landsgrenzen houden, zijn er knelpunten door rechtshulpverzoeken en verschillen in wetgeving.
Uit de interviews blijkt dat politiemensen zich bewust zijn van de toestemming van de officier van justitie die regelmatig nodig is bij het gebruik van digitale sporen. Dit wordt niet zozeer gezien als belemmering. De knelpunten door het internationale karakter van digitale sporen worden erkend door de geïnterviewden.

Uit de literatuur over het vierde thema – de mentale factoren – komen belemmerende factoren naar voren als onzekerheid, werkstress, angst voor het maken van fouten en een gebrek aan interesse. Ook zou er meer waarde worden gehecht aan traditionele sporen dan aan digitale sporen, is vergrijzing een aandachtspunt en is de steun van leidinggevenden een belangrijke stimulerende factor.
Lang niet al deze factoren worden vanuit de interviews bevestigd. Hoewel een gebrek aan interesse en steun van leidinggevenden wordt erkend, ziet men een duidelijke beweging richting het toedichten van steeds meer waarde aan digitale sporen. Tot slot zou veranderbereidheid volgens de geïnterviewden belangrijker zijn in het verklaren van het gebruik van digitale sporen dan de leeftijd van politiemedewerkers.

Een bondig antwoord op de vraag 'Welke niet-technische factoren belemmeren het tactisch gebruik van digitale sporen door politiemensen?' is op basis van de bevindingen dat er nog steeds sprake is van een gebrek aan kennis en capaciteit. Daarnaast zijn er sterke twijfels over de effectiviteit van bestaande opleidingen. Verouderde en/of versnipperde informatie op intranet is een belemmering, net als de tijd die het kost om

grote hoeveelheden data te onderzoeken. Door het internationale karakter van digitale sporen is er vertraging in juridische processen. Een gebrek aan interesse en veranderbereidheid bij politiemensen vormt een belemmering. Tot slot wordt de beperkte steun van leidinggevenden als knelpunt gezien.

Resultaten uit het casusonderzoek
Op basis van bovengenoemde knelpunten en mogelijkheden zijn er over deze factoren stellingen voorgelegd aan de respondenten van het casusonderzoek. Hieruit blijkt dat zij zich deels kunnen vinden in de genoemde (on)mogelijkheden. Duidelijk is dat de potentie van digitale sporen wordt ingezien. Men herkent zich dan ook niet in een gebrek aan interesse als knelpunt. Verder is bijna twee derde het eens met de stelling dat digitale sporen betrouwbaar zijn. De omvangrijkheid van digitale sporen ziet men echter wel als knelpunt, net als een gebrek aan capaciteit. Een kleinere groep (ongeveer een derde) weet niet hoe ze met digitale sporen moet werken.
Over de overige knelpunten dan wel mogelijkheden zijn de meningen verdeeld: er is geen duidelijke conclusie te trekken over wat respondenten vinden van factoren als faciliteiten, gebruiksvriendelijkheid van digitale sporen, onzekerheid over eigen kennis, inzicht in bevoegdheden en de bekendheid met de mogelijkheden van digitale sporen. Hieruit kan worden afgeleid dat deze knelpunten niet manifest zijn en tegelijk ook nog niet volledig zijn weggenomen in de politieorganisatie.

7.2 Gebruik van (digitale) sporen: resultaten uit casusonderzoek en vragenlijst

In deze paragraaf beantwoorden we de tweede onderzoeksvraag: 'In hoeverre en op welke wijze gebruiken politiemensen digitale sporen bij opsporingsonderzoek?' Aan 76 respondenten is een casus voorgelegd waarbij tien keuzes gemaakt moesten worden tussen ofwel een digitaal ofwel een analoog bewijsstuk om de casus op te lossen. De respondenten waren voornamelijk werkzaam in de Eenheid Noord-Nederland en 40 procent van hen werkt veel dan wel uitsluitend met zaken op het gebied van digitale criminaliteit. De keuzes en bijbehorende toelichtingen kunnen daardoor gekleurd en minder representatief zijn voor alle politiemensen in Nederland (zie ook hoofdstuk 8 en bijlage 5). Respondenten kiezen, zo blijkt, met name op basis van de informatie uit de casus voor een digitaal dan wel analoog bewijsstuk. Onafhankelijk van de aard van het bewijsstuk wordt derhalve gekozen voor het bewijsstuk dat zij het meest nuttig achten om de casus stapsgewijs op te lossen. Zo wordt geredeneerd dat het bewijsstuk kan helpen bij het inzichtelijk maken van contacten van de verdachte of het kan bijvoorbeeld inzicht geven in details van het letsel van het slachtoffer.

Wanneer aan respondenten werd gevraagd waarom ze een bepaalde keuze maken, is er overlap tussen de keuze voor een digitaal dan wel analoog bewijsstuk. Bij zowel een keuze voor digitaal als analoog zegt men dat het bewijsstuk meer oplevert, betrouw-

baarder en/of concreter is. Deze eigenschappen kunnen derhalve niet worden toegedicht aan een type bewijsstuk.

Bij het kiezen voor een digitaal bewijsstuk wordt de vergankelijkheid genoemd. Men voorkomt met deze keuze dat het bewijsstuk later niet meer kan worden geraadpleegd. Daarnaast zou een digitaal bewijsstuk gemakkelijker zijn om in te zoeken en kan de informatie later worden gebruikt in een verhoor. Laatstgenoemde laat zien dat digitaal en analoog elkaar kunnen versterken.

Analoge sporen, zoals een verhoor of getuigenverklaring, werden gekozen uit nieuwsgierigheid en omdat het de mogelijkheid biedt om dóór te vragen. Daarnaast zou het direct en snel informatie bieden. Dit kwam ook terug in een interview in hoofdstuk 4: het is makkelijker voor het rondmaken van een zaak om simpelweg uit een verhoor te halen dat A en B vrienden zijn, dan dat dit moet worden vastgesteld uit digitale bronnen.

Gemiddeld genomen werd 6,3 van de tien keer gekozen voor het digitale bewijsstuk en 3,7 keer voor het analoge bewijsstuk. Er lijkt een lichte voorkeur te zijn het voor digitale sporen. Verschillen tussen groepen zijn er amper. Slechts bij één keuze kozen vrouwen significant vaker dan mannen voor het open bronnenonderzoek (digitaal) dan voor het verhoor (analoog). Twee keuzes lieten zien dat er significante verschillen waren tussen leeftijdscategorieën. In beide gevallen koos de groep van 51 jaar of ouder het vaakst voor het digitale bewijsstuk. Dit geldt ook overkoepelend voor alle tien keuzes: de oudste groep van 51 jaar of ouder kiest het vaakst voor een digitaal bewijsstuk (7,2 keer) en de jongste groep tot 30 jaar het minst (5,4 keer). Ervaring met zaken op het gebied van digitale criminaliteit of het volgen van een opleiding en/of cursus zorgt er niet voor dat men daardoor vaker voor een digitaal spoor kiest.

Handelingsstrategieën van respondenten bij het gebruiken van digitale sporen richten zich onder andere op het inschakelen van de benodigde expertise. Gelet op het onderzoek van Van Valkengoed (2017) is dit een positieve bevinding. Desalniettemin gaat een groep respondenten liever zelf aan de slag met het bewijsstuk. Bijvoorbeeld door naar de loggegevens te kijken of onderzoek te doen naar een IP-adres. Hierbij worden juridische overwegingen aangehaald, waarbij men noemt dat bijvoorbeeld vorderingen dienen te worden ingediend bij Facebook of dat toestemming nodig is voor het uitlezen van een smartphone. De grenzen van wanneer wetgeving wordt overtreden zijn echter niet altijd helder, net als de risico's van het achterlaten van digitale voetafdrukken door de politie zelf. Er wordt bijvoorbeeld ook op de eigen werkplek naar digitale sporen gezocht. Hier komen we later op terug.

In de toelichtingen op de vraag wat de ervaring is van respondenten met digitale sporen in het algemeen, blijkt dat ze over het algemeen de mogelijkheden inzien van digitale sporen. Dat de politie nog niet daar is waar zij zou moeten zijn, wordt erkend,

maar er is een trend waarneembaar in de groei van bewustwording van digitale mogelijkheden in opsporingsonderzoek. Uit de toelichtingen van de groep met inmiddels redelijk wat ervaring met digitale sporen komt naar voren dat zij de komende jaren kunnen doorgroeien in hun kennis en vaardigheden. Juist doordat ze mogelijkheden verkennen, zien ze in dat kansen beter kunnen worden benut wanneer digitale sporen in de praktijk worden gebruikt.

Een kort antwoord op de vraag 'In hoeverre en op welke wijze gebruiken politiemensen digitale sporen bij opsporingsonderzoek?' luidt gezien het vorenstaande dat respondenten in ons onderzoek vaker voor een digitaal dan voor een analoog spoor kiezen. Handelingsstrategieën richten zich op het inschakelen van de benodigde digitale expertise om het spoor te kunnen duiden. Daarnaast gaat een groep respondenten liever zelf aan de slag met het digitaal bewijsstuk. Het algemene beeld van de respondenten over het gebruik van digitale sporen bij opsporingsonderzoek is dat er nog veel te leren is en de politieorganisatie nog niet daar is waar het moet zijn, maar dat er een trend waarneembaar is in de groei van bewustwording van de mogelijkheden die digitale sporen kunnen bieden.

7.3 Intentie en daadwerkelijk gebruik van digitale sporen

In deze paragraaf beantwoorden we de derde onderzoeksvraag: 'In hoeverre hebben politiemensen de intentie om digitale sporen te gebruiken bij opsporingsonderzoek en in hoeverre handelen ze naar hun intenties?' Uit het vragenlijstonderzoek blijkt dat respondenten de intentie hebben om digitale sporen te gebruiken wanneer ze aan een zaak werken. Slechts iets minder dan een vijfde van de respondenten heeft een lage score op intentie voor het gebruik van digitale sporen. Bij de vraag in hoeveel van tien zaken men verwacht digitale sporen te gebruiken, schat men in dat dit om 6,4 zaken gaat (64%). Ook een maand na het casusonderzoek, toen gevraagd werd in hoeveel procent van de zaken de afgelopen maand gebruik was gemaakt van digitale sporen, zien we ongeveer hetzelfde antwoord als bij intenties: gemiddeld hadden de 31 respondenten die deze vraag hadden beantwoord in 62,1 procent van de zaken gebruikgemaakt van digitale sporen. Er is echter geen significant verband vastgesteld tussen de intentie om digitale sporen te gebruiken en het daadwerkelijke gebruik ervan.
Het lijkt erop dat men in opsporingsonderzoek inmiddels vaker een digitaal bewijsstuk gebruikt dan een analoog bewijsstuk. Er is echter sprake van spreiding. Zo waren er drie respondenten die in een maand tijd in geen enkele zaak digitale sporen hadden gebruikt en twaalf respondenten die in alle zaken digitale sporen hadden gebruikt.

Er zijn significante, maar zwakke verbanden gevonden tussen de intentie tot het gebruik van digitale sporen en minder angst voor het maken van fouten, dan wel minder onbekendheid met de mogelijkheden van digitale sporen. Er is meer intentie tot het gebruik van digitale sporen wanneer respondenten inschatten dat ze met digitale sporen kunnen werken. Daarnaast bleek dat het daadwerkelijke gebruik van digitale spo-

ren hoger is wanneer respondenten inschatten dat ze weten hoe ze met digitale sporen moeten werken en indien respondenten vinden dat het werken met digitale sporen gebruiksvriendelijk is.

Tot slot is er geen invloed van de belangrijkste factoren uit hoofdstuk 4 – zoals betrouwbaarheid van digitale sporen, beschikbare capaciteit en angst voor het maken van fouten – op het verband tussen de intentie om digitale sporen te gebruiken en het daadwerkelijke gebruik ervan.

Gezien de bevindingen luidt het korte antwoord op de vraag 'In hoeverre hebben politiemensen de intentie om digitale sporen te gebruiken bij opsporingsonderzoek en in hoeverre handelen ze naar hun intenties?' als volgt: politiemensen hebben de intentie om digitale sporen te gebruiken, maar er is geen significant verband tussen deze intentie en het daadwerkelijk gebruik ervan. Politiemensen handelen derhalve niet naar hun intenties. Desalniettemin gebruiken respondenten in gemiddeld 62,1 procent van hun zaken digitale sporen. Laatstgenoemde bevinding is echter onderzocht met kleine respondentaantallen, waardoor we er geen directe conclusies aan kunnen verbinden.

7.4 Slotoverwegingen

Uit het onderzoek blijkt dat politiemensen welwillend zijn ten aanzien van het gebruik van digitale sporen en ook de intentie daartoe hebben. Ze zien het nut van digitale sporen in en zijn veelal in staat om te bepalen welke vragen gesteld moeten worden om de sporen te gebruiken voor het oplossen van een casus. Voor het beantwoorden van deze vragen is (ook bij twijfel) echter expertise nodig. Ze hebben veelal zelf nog niet de benodigde kennis en ervaring om met (alle) digitale sporen aan de slag te gaan. Uit de interviews en het literatuuronderzoek blijkt dat de benodigde digitale expertise die zij zouden willen inschakelen, volgens hen niet altijd beschikbaar is.

Verder komt naar voren dat specialisten benaderbaar dienen te zijn. In Leeuwarden is men bijvoorbeeld zeer te spreken over de toegankelijkheid van het digitaal platform: rechercheurs kunnen direct met hun probleem naar de desbetreffende experts lopen en verder met hun zaak. Op andere locaties, waar dit niet zo georganiseerd is, loopt men tegen barrières aan. Er is te weinig capaciteit voor de 'vraagbaak-functies' en expertise is niet voldoende toegankelijk. Bovendien weten politiemensen niet altijd welke expert ze bij welke vraag aan de jas moeten trekken.

De vraag voor de politieorganisatie is of deze conclusie dient te worden toegepast in toekomstig beleid: óf er wordt vastgehouden aan het steeds verder versterken van het kennisniveau in alle lagen van de politieorganisatie over cybercrime/digitaal zodat alle politiemedewerkers steeds vaker zelf met digitale sporen aan de slag kunnen gaan, óf er wordt gekozen voor het aantrekken van (nog) meer gemakkelijk te benaderen specialisten die in staat en beschikbaar zijn om vragen van collega's te beantwoorden. Dit

vraagt om een duidelijke balans tussen de vragen die er zijn, wat van politiemensen zelf verwacht mag worden en de capaciteit van experts om te helpen die vragen te beantwoorden.

Een gebrek aan kennis is en blijft een belangrijke belemmerende factor bij het gebruik van digitale sporen door politiemedewerkers. Er zijn steeds meer specialisten, maar lang niet alle respondenten kunnen met de digitale sporen uit het casusonderzoek zelf aan de slag. Een deel heeft geen enkele cursus gevolgd op het gebied van cybercrime/digitaal. Indien er wel cursussen zijn gevolgd, gaat het fout bij het blijven oefenen en toepassen van de opgedane kennis, waardoor de kennis niet beklijft. Respondenten vinden dat zelf ook jammer, zo blijkt uit de gegeven toelichtingen. Politiebeleid dient zodoende niet alleen gericht te zijn op het stimuleren van opleidingen, maar ook op het vasthouden van opgedane kennis in de dagelijkse praktijk.

Daarnaast zijn er risico's blootgelegd bij het gebruik van digitale sporen. Daarbij vallen twee risico's met name op. Ten eerste de omschrijving van respondenten dat dergelijke sporen "niet liegen", betrouwbaar zijn en daarmee objectiever dan analoge sporen. Digitale sporen zijn echter gemakkelijk te manipuleren. Dit geldt bijvoorbeeld voor tijdsaanduidingen, loggegevens, foto's, filmpjes en verstuurde berichten. Hoewel vaak achterhaald kan worden in hoeverre sporen gemanipuleerd zijn, dient men altijd alert te zijn op de interpretatie ervan. Politiemensen kunnen er niet zonder meer vanuit gaan dat digitale sporen waarheidsgetrouw zijn. Dit kan kwalijke gevolgen hebben voor (de vervolgstappen in) een zaak. De bewustwording hiervan is belangrijk.

Ten tweede zijn er risico's ten aanzien van de juridische stappen die gezet moeten worden om digitale sporen te gebruiken. Het vereiste juridische kader wordt niet door alle politiemensen toegepast. In het casusonderzoek komt naar voren dat politiemensen bijvoorbeeld 'even kijken' wat er online te vinden is over een verdachte. Dit gebeurt soms vanaf een normale werkplek, in tegenstelling tot een beveiligde (iRN-)omgeving. Hoewel een zoekactie in open bronnen een geringe inbreuk op de privacy oplevert, betekent dit niet dat er op systematische wijze open bronnen mogen worden doorzocht. Een schending kan bovendien nadelige gevolgen hebben voor de vervolging van verdachte(n). Daarnaast kan online 'rondneuzen' vanaf een normale werkplek het risico inhouden dat een verdachte ontdekt dat de politie interesse heeft in hem of haar. Eén van de respondenten vertelde dat hij/zij voor opsporingsdoeleinden een fakeaccount gebruikt. We hebben de details hiervan niet onderzocht. Mogelijk gaat het om een officiële politietool; mogelijk is het een individueel initiatief. Wat de mogelijkheden van politiemensen zijn in dit verband, lijkt hoe dan ook een goede vraag voor een (juridisch) vervolgonderzoek.

Vergrijzing van de politieorganisatie lijkt geen negatieve rol te spelen bij het gebruik van digitale sporen. Gemiddeld kiest de oudste groep van 51 jaar of ouder het vaakst voor een digitaal bewijsstuk in ons onderzoek (met 7,2 van de tien keer). Dit zien we

ook bij de resultaten uit de interviews: het gaat eerder om de veranderbereidheid van een politiemedewerker. Die factor is dus kennelijk belangrijker, ongeacht de leeftijd. In vervolgonderzoek zou nader kunnen worden ingezoomd op deze factor; eventueel in combinatie met onderzoek naar de veranderbereidheid van politiemedewerkers.

Hoewel het onderzoek laat zien dat er stappen gemaakt zijn in de bewustwording van het belang van digitale sporen en de kansen die hierdoor benut kunnen worden, is er nog steeds een groep met te weinig kennis om digitale sporen daadwerkelijk te gebruiken – ook al erkennen ze het belang ervan en ook al hebben ze de intentie om er wat mee te doen. Bovendien handelen politiemensen niet altijd naar hun intenties. Laatstgenoemde is echter onderzocht met een kleine groep respondenten en het verdient aanbeveling om dat in een vervolgonderzoek verder uit te diepen.

8. Beperkingen van het onderzoek

Het onderzoek kent een aantal beperkingen. Hoewel is getracht in de oproep voor het casusonderzoek geen vermelding te maken van 'digitaal' dan wel 'cybercrime', is er toch gesproken over digitale sporen in de oproep die op intranet is geplaatst in de Eenheid Noord-Nederland. In totaal waren 56 van de 76 respondenten in het casusonderzoek werkzaam bij de Eenheid Noord-Nederland. Dertig van deze 56 respondenten hebben veel dan wel uitsluitend met zaken op het gebied van digitale criminaliteit te maken gehad. Hieruit blijkt dat de oproep mogelijk ertoe heeft geleid dat politiemensen met affiniteit voor cybercrime/digitaal zich hebben aangemeld voor het casusonderzoek en daardoor de keuzes en toelichtingen gekleurd en minder representatief zijn voor alle politiemensen in Nederland. Hier staat tegenover dat deze respondentenwerving er mogelijk aan heeft bijgedragen dat we ook opvattingen en inzichten hebben kunnen noteren van politiemensen die veel ervaring hebben met het gebruik van digitale sporen (zie paragraaf 5.4).

De zes rechercheurs die zijn geïnterviewd – deels ter beantwoording van de eerste deelvraag – waren allen werkzaam bij de Eenheid Noord-Nederland. Hierdoor kunnen deze resultaten mogelijk niet gegeneraliseerd worden naar overige eenheden. Daarnaast is het aantal respondenten dat deelnam aan het casusonderzoek klein. Bij het onderzoek naar intenties en gedrag is gebruikgemaakt van een groep van 31 respondenten. Dit is een laag aantal, op basis waarvan we geen verstrekkende conclusies mogen trekken. Hoewel dit beperkingen zijn, moet worden opgemerkt dat de studie verkennend van aard is en niet tot doel had om generaliseerbaar te zijn.

In dit onderzoek is gekozen voor een minder gangbare onderzoeksmethode. In het casusonderzoek werden respondenten gedwongen een keuze te maken tussen een digitaal dan wel een analoog bewijsstuk. Hoewel in het voorbereidingstraject twee politiemensen zijn betrokken bij de ontwikkeling van de casus en getracht is de keuzes zo gelijk mogelijk aan elkaar te maken, is het onmogelijk gebleken altijd exact gelijkwaardige keuzes van digitale dan wel analoge aard aan de respondenten voor te leggen. Diverse malen in het casusonderzoek zeiden respondenten dat ze normaal gesproken beide bewijsstukken zouden kiezen. Logischerwijs is dat in opsporingsonderzoek ook altijd mogelijk en komt het casusonderzoek hierdoor niet overeen met de werkelijkheid.

Ook bij de keuze voor bijvoorbeeld de verklaring van een arts enerzijds en een geluidsopname op een smartphone anderzijds werd gezegd dat voor de verklaring van de arts gekozen móést worden, omdat dit voorwaardelijk is voor de opbouw van het dossier. Alsnog koos overigens bijna 70 procent niet voor deze verklaring. Desalniettemin heeft het casusonderzoek, juist doordat respondenten werden gedwongen te kiezen, inzicht kunnen geven in de waarde die aan bewijsstukken wordt toegekend en voorkeuren voor bepaalde bewijsstukken.

Verder is het de vraag of met dit onderzoek is gemeten wat we wilden meten. Keuzes kunnen zijn gemaakt op basis van de casus, zoals ook in toelichtingen werd gezegd. In de casus zitten digitale elementen, wat ook door respondenten wordt genoemd als reden waarom ze een bepaalde keuze maken. Bijvoorbeeld bij keuze 1, waarbij Instagram zowel in de casus als in de digitale keuze wordt genoemd. Voor respondenten is mogelijk duidelijker wat een analoog spoor gaat opleveren dan een digitaal spoor. Een digitaal spoor kent veelal meer randvoorwaarden en is daardoor complexer. Door bij iedere keuze aan de respondenten te vragen toe te lichten waarom een keuze is gemaakt, is getracht zo transparant mogelijk te zijn in de rapportage.

In vervolgonderzoek kan meer variatie worden aangebracht in de keuze voor een digitaal dan wel analoog bewijsstuk. Er was nu sprake van enige overlap in keuzes voor social media en informatie van buren. Daarnaast gaven respondenten zoals gezegd aan dat het feit dat de casus zich in de digitale wereld afspeelt, voor hen een reden was om voor een digitaal bewijsstuk te kiezen. In een vervolgonderzoek zouden meerdere experimentele situaties kunnen worden voorgelegd en kan een controlegroep worden gebruikt. Verder zou randomisatie in keuzemogelijkheden en -uitkomsten kunnen bijdragen aan de zuiverheid van de onderzoeksuitkomsten.

Bovenstaande beperkingen nemen niet weg dat met dit onderzoek een eerste, verkennende stap is gezet in het beter begrijpen van motivaties in het wel of niet gebruik maken van digitale sporen. Toekomstige studies kunnen bijdragen aan het verder ontwikkelen van deze kennis door rekening te houden met de gepresenteerde beperkingen.

Literatuurlijst

ACPO. (2011). *Managers Guide - Good Practice and Advice for Managers of e-crime investigation*. London. Retrieved from http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf

Armitage, C.J. & Connor, M. (2001). Efficacy of the theory of planned behavior: A meta-analytic review. *British Journal of Social Psychology, 40,* 471-499.

Brown, C.S.D. (2015). Investigating and prosecuting cybercrime: forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, 9(1), 55-119.

Bryant, R. & Bryant, S. (2014). *Policing Digital Crime*. Ashgate.

Blaas, J. (2015). *ICT hulpmiddelen voor de generalist in de opsporin*g. Hogeschool van Amsterdam.

Baar, R.B. van, Beek, H.M.A. van & Eijk, E.J. van (2014). Digital forensics as a service: a game changer. *Digital Investigation*, 11, S54-62.

Casey, E. (2011). *Digital Evidence and Computer Crime* (3rd ed.). Amsterdam: Elsevier Academic Press.

Custers, B. (2012). Technology in policing: Experiences, obstacles and police needs. *Computer Law & Security Review*, 28, 62-68.

Daniel, L.E. & Daniel, L.E. (2012). *Digital Evidence Is Everywhere*. Waltham: Elsevier. http://doi.org/10.1016/B978-1-59749-643-8.00001-8

Domenie, M., Leukfeldt, R., Wilsem, J. van & Stol, W.Ph. (2012). Slachtofferschap van cybercrime in kaart gebracht. *Tijdschrift Voor Veiligheid, 11*(2), 47–56.

Edison, S.W. & Geisler, G.L. (2012). Measuring attitudes towards general technology: Antecedents, hypotheses, and scale development. *Journal of Targeting, Measurement and Analysis for Marketing*, 12(2), 137-156.

Ernst, S., Veen, H. ter, Lam, J. & Kop, N. (2019). *Leren van technologisch innoveren: "De techniek is niet zo spannend".* Apeldoorn: Politieacademie.

Flory, T.A.C. (2016). Digital forensics in law enforcement: a needs based analysis of Indiana agencies. *Journal of Digital Forensics*, *11*(1), 7-38.

Fishbein, M. & Ajzen, I. (2010). *Predicting and changing behavior*. New York: Psychology Press. http://doi.org/10.4324/9780203937082

Gritter, E. (2016). Opsporing in de digitale wereld: Het onderzoek van in beslag genomen gegevensdragers. *Delict & Delinquent, 43*, 493-503.

Haenen, M. (2015, September 5). Recherchewerk politie gehinderd door "te weinig kennis en ervaring." *NRC*. Retrieved from https://www.nrc.nl/nieuws/2015/09/05/recherchewerk-politie-gehinderd-door-te-weinig-kennis-en-ervaring-a1413419

HMIC (Her Majesty's Inspectorate of Constabulary) (2014). *The Strategic Policing Requirement. An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement.* London: HMIC.

Holt, T.J. & Bossler, A.M. (2012). Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments. *Cyberpsychology, Behavior, and Social Networking, 15*(9), 464-472.

Huisman, S., Princen, M., Klerks, P. & Kop, N. (2016). *Handelen naar waarheid.* Amsterdam.

Junger, M., Montoya, L., Hartel, P. & Karemaker, M. (2013). *Modus operandi onderzoek naar door Informatie en Communicatie Technologie (ICT) gefaciliteerde criminaliteit*. Enschede. Retrieved from http://www.websitevoordepolitie.nl/archief/politiewerk-na-de-digitale-revolutie-706.html

Koops, B.J. (2012). Politieonderzoek in open bronnen op internet: Strafvorderlijke aspecten. *Tijdschrift voor Veiligheid 11*(2), 30-46.

Lewig, K.A. & Dollard, M.F. (2003). Emotional dissonance, emotional exhaustion and job satisfaction in call centre workers. *European Journal of Work and Organizational Psychology*, *12*(4), 366-292.

MacNeil, T.L. (2015). *Police Opinions of Digital Evidence Response Handling in the State of Georgia: An Examination from the Viewpoint of Local Agencies' Patrol Officers*. ProQuest Dissertations and Theses.

Odinot, G., Jong, D. & Leij, J. van der (2012). *Het gebruik van de telefoon-en internettap in de opsporing*. Retrieved from http://repository.tudelft.nl/view/wodc/uuid:a4b1041c-0af4-4b30-bca2-ecc28dd79c8d

Rassin, E. (2015). *De diagnostische waarde van bewijs.* Deventer: Wolters Kluwer.

Rompu, P. van (2015). *"A cat-and-mouse game": The fight against cyber stalking in the Netherlands*. Utrecht University.

Skogan, W.G. (2008). Why reforms fail. *Policing and Society, 18*(1), 23-34.

Stevens, L. (2017). Onderzoek in een smartphone: Zoeken naar een redelijke verhouding tussen privacybescherming en werkbare opsporing. *Ars Aequi, september*, 730-735.

Stol, W.Ph. (2004). Trends in cybercrime. *Justitiële Verkenningen, 8,* 22–23.

Stol, W.Ph. & Jansen, J. (2013). *Cybercrime and the police*. The Hague: Eleven International Publishing.

Stol, W.Ph., Leukfeldt, E.R. & Klap, H. (2013). In W.Ph. Stol & J. Jansen (Eds.), *Cybercrime and the police*. (pp. 61-74). The Hague: Eleven International Publishing.

Stol, W.Ph. & Strikwerda, L. (2017). *Strafrechtspleging in een digitale samenleving*. Den Haag: Boom Juridisch.

Stol, W.Ph. & Strikwerda, L. (2018). Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving. *Tijdschrift voor Veiligheid, 17*(1-2), 8-22.

Valkengoed, T. van (2017). *Competentieonderzoek Cybercrimeopsporing*. Apeldoorn: Politieacademie.

Veenstra, S., Zuurveen, R., Kerstens, J. & Stol, W.Ph. (2015). Focusgroepbijeenkomsten in het kader van de handreiking "Opsporing in een gedigitaliseerde samenleving". Leeuwarden: Onderzoeksgroep Cybersafety.

Veenstra, S., Zuurveen, R. & Stol, W.Ph. (2015). *Cybercrime onder bedrijven: Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland.* Leeuwarden: Lectoraat Cybersafety.

Veenstra, S., Zuurveen, R., Kerstens, J. & Stol, W.Ph. (2016). *Opsporing in een gedigitaliseerde samenleving.* Leeuwarden: Lectoraat Cybersafety.

Bijlage 1. **Interviewprotocol**

Interviewprotocol benutten van digitaal bewijsmateriaal

Achtergrond en toelichting (1)

1. Onderzoeker stelt zichzelf voor…
2. Doel van onderzoek (en achtergronden)
3. Tijdsduur (ongeveer een uur)
4. Afbakening – beperking tot digitale sporen (definitie)*
5. Verwerking gegevens anoniem (mag naam genoemd worden in rapport?)*
6. Toestemming voor opname (daarna start interview)
7. Opbouw interview (korte toelichting)

Inleidende vragen (2)

– Zou u zich kort kunnen voorstellen en uw functie kunnen toelichten?
– Welke rol spelen digitale sporen in uw dagelijks werk? Maakt u gebruik van digitale sporen? Wat voor soort sporen? Hoe vaak?

Meerwaarde en knelpunten bij het gebruik van digitale sporen (3)

Persoonlijke motivaties

– Wat zijn voor u redenen om digitale sporen te gebruiken in uw werk?
– Wat zijn voor u redenen of omstandigheden om digitale sporen niet of minder snel te gebruiken in uw werk?
(onderzoeker noteert knelpunten).

Motivaties van collega's

– Wat zijn voor uw collega's redenen om digitale sporen te gebruiken in hun werk?
– Wat zijn voor uw collega's redenen of omstandigheden om digitale sporen niet of minder snel te gebruiken in uw werk?
(onderzoeker noteert(eventueel) aanvullende knelpunten).

Rangschikking

– Zou u de volgende kaartjes (op basis van knelpunten) kunnen rangschikken en beginnen met het voor u belangrijkste knelpunt en eindigen met de minst belangrijke?

Factoren uit de literatuur – open starten daarna concreet maken (4)
In de literatuur en uit eerder onderzoek van de Onderzoeksgroep Cybersafety zijn knelpunten naar voren gekomen die mogelijk verhinderen dat digitale sporen worden gebruikt. Zou u kunnen aangeven of u dit knelpunt herkent in uw dagelijks werk en kunnen toelichten waarom dit in uw ervaring al dan niet een knelpunt is?
Eerst zal ik u vragen naar knelpunten binnen een bepaald thema, vervolgens zal ik concreet knelpunten benoemen en aan u vragen of u deze knelpunten herkent.
Probeer voorbeelden te noemen die ze zelf al hebben genoemd in eerste instantie om deze aspecten toe te lichten (!)

1. **Praktisch organisatorisch/kennistekort** (werkomgeving)
2. **Juridische knelpunten** (wetgeving)
3. **Forensisch-technische knelpunten** (aard van de sporen)
4. **Mentale factoren** (psychische of persoonlijke factoren)

Afsluiting (5)

1. Aan het begin van het interview heeft u een rangschikking gemaakt op basis van de door u genoemde knelpunten.

   Later in het gesprek zijn nog enkele aanvullende knelpunten naar voren gekomen. Zou u nu aan het einde van dit gesprek tot dezelfde rangschikking komen of zou u nog iets willen bijstellen of aanpassen? (wat en waarom?)

2. Is er nog iets wat niet aan bod is gekomen en wat u graag kwijt zou willen over dit thema of dit onderzoek?

3. Een vervolgstap op de interviews is het laten deelnemen van collega's (X) aan een concrete casus (experiment) waarbij er zowel digitale sporen als traditionele sporen aanwezig en te gebruiken zijn. We starten begin 2019 met de ontwikkeling daarvan. Zouden we u mogen benaderen om mee te denken en/of feedback te geven op de door ons bedachte casus?

4. Hartelijk dank voor uw medewerking!

Gebruiken bij vragenblok 4:

– Kennistekort:
  - Niet weten wat men zoekt/ongerichte verzoeken experts en providers.
  - Niet de potentie en mogelijkheden zien van digitaal bewijs.
  - Moeilijk te interpreteren bewijsmateriaal/vertaalslag in bruikbare vorm.
  - Gebrek aan overzicht van beschikbare technologie en mogelijkheden.
– Praktische/organisatorische obstakels:
  - Faciliteiten (uitleesstations en iRN-computers, etc).
  - Delen van informatie (intranet werkt niet)/kennis versnippert aanwezig.
  - Digitale experts overvraagd (oplossing is meer accent bij onderzoeker).
  - Vluchtigheid van digitale sporen (snelheid nodig, lukt niet altijd).
  - Bewaartermijn van gegevens.
  - Vertraging door samenwerking met providers e.d en buitenland.
  - Aan wie binnen organisatie verzoek richten?
  - IP-adressen moeilijk te achterhalen.
  - Financiering, budget en capaciteit voor innovatie.
  - Administratieve last bij onderzoeken (voorstel centrale dienst die dat overneemt).
  - Onvoldoende sturing en management.
  - Aanpassingsvermogen van collega's.
  - Voorkeuren van de teamleider.
  - Efficiëntie door gebruik van systemen zoals Hansken en Trackinspector?
  - Gebruiksvriendelijkheid van software/diensten.
  - Gebrek aan systematiek/standaardisatie van werkwijze?
– Juridisch:
  - Wettelijke basis voor gebruik technologie (smartphone-arrest).
  - Traagheid door verzoeken aan officier van justitie.
  - Onduidelijkheid over wat kan en mag, kan reden zijn om niets te doen.
  - Gebrek aan jurisprudentie om van te leren.
  - Weigering van rechters en Openbaar Ministerie van digitaal bewijs (lijkt me ook praktisch).
  - Eerder: ook buitenlandse providers en jurisdictie kan probleem zijn.
– Mentale factoren (komen grotendeels overeen met ANPR-studie):
  - Onzekerheid/werkstress/gebrek aan interesse in technologie.
  - Het bekende eerder kiezen dan het onbekende.
  - Ideeën en overtuigingen over waarde bewijsstuk (makkelijk te manipuleren, gefabriceerde data, etc.).
  - Vergrijzing (leeftijd) maakt dat zaken met digitale component blijven liggen.
  - Zelfs gebruik open bronnen (iRN) niet vanzelfsprekend.
  - Bang om onderzoeken te verprutsen.
  - Elkaar niet durven aan te spreken op onkunde: "Kritiek wordt al snel persoonlijk opgevat als iemands professionaliteit in twijfel wordt getrokken."
  - Taken niet bij hun werk vinden passen.

- Onzeker over eigen kennisniveau, behoefte aan training (leidt het volgen van een training tot daadwerkelijk meer kennis?)
- Teamgrootte: hoe groter het team, hoe groter de kans dat kennis over digitaal aanwezig is en digitaal eerder 'normaal' is.
- Een politieagent krijgt meer erkenning bij het (met succes) gebruiken van traditionele sporen, dan bij het gebruiken van digitale sporen.
- Het gebruiken van digitale sporen wordt gezien als zonde van de tijd ('drains valuable resources'); tijd die beter aan traditionele sporen gewijd zou kunnen worden.
- Steun van leidinggevende om digitale sporen te gebruiken.
- Steun van collega's (aanjagers) om digitale sporen te gebruiken.

Bijlage 2. **Casusonderzoek**

Eva doet aangifte van zware mishandeling, diefstal van haar telefoon (met braak) en smaad. Eva vertelt dat ze op 14 januari 2019 ruzie kreeg met haar toenmalige vriend Tony. Het was een heftige ruzie waarbij zowel Eva als Tony naar elkaar zouden hebben geschreeuwd. Tony zou op een gegeven moment Eva hard in het gezicht hebben geslagen met een hard voorwerp en er vandoor zijn gegaan. Mét haar telefoon, zo bleek later. Eva had als gevolg van de zware mishandeling haar kaak gebroken en moest worden geopereerd.

Zonder toestemming van Eva zou Tony met behulp van haar inlogcode toegang hebben verkregen tot haar telefoon en zou hij een naaktfoto van Eva die op haar telefoon stond op Instagram hebben geplaatst. Tony zou Instagram vervolgens weer hebben uitgelogd, zodat Eva op haar telefoon (toen ze hem weer in beheer had) geen meldingen kreeg over de geposte naaktfoto. Daar moesten haar vriendinnen haar op een later moment op attenderen. Daarnaast zou Tony 500 euro met de ING-app van Eva overgemaakt hebben naar de rekening van ene Henk Elands. Eva vermoedt, onder andere doordat ze weet dat Tony diverse keren is gebeld door andere vrouwen, dat zij niet het enige slachtoffer is.

Digitaal	**Analoog**
Resultaten van een analyse van de contacten van Eva in haar (openbare) Instagram- en Facebookaccounts.	Resultaten van een buurtonderzoek in de omgeving van de plaats delict.
Op een geplaatste foto op Instagram is zichtbaar dat Tony, Henk en Roy samen op de foto staan. Tony leunt met zijn handen op de schouders van Henk en Roy. Alle drie lachen.	Buurtbewoners op nummer 53 en 61 hebben Tony, Henk en Roy op het adres van het slachtoffer gezien. Ze waren aan het lachen en Tony had een arm of hand op de schouders van Henk en Roy gelegd.
Hieruit blijkt dat Tony vriendschappelijke contacten onderhoudt met Henk Elands.	

Digitaal	**Analoog**
Open bronnenonderzoek (social media, fora, YouTube, etc.) op de nickname van Tony: 'Tonzone'.	Verhoor van Roy, vriend van verdachte Tony.
Voor dit onderzoek is de komende twee weken geen iRN-computer beschikbaar, waardoor een analyse (nog) niet mogelijk is.	Roy is twee weken op vakantie naar Barcelona, waardoor een verhoor (nog) niet mogelijk is.
Hieruit kunnen geen conclusies worden getrokken.	

Digitaal	Analoog
De modem en router van Eva worden veiliggesteld en uitgelezen.	Getuigenverklaring van de overbuurman van Eva op nummer 52.
Hieruit blijkt dat de telefoon van Tony om 15 uur (rond het tijdstip van het delict) verbinding heeft gemaakt met het thuisnetwerk van Eva.	De getuige verklaart dat hij Tony om 15 uur (rond het tijdstip van het delict) in het huis van het slachtoffer heeft gezien.
Hieruit blijkt dat verdachte Tony rond het tijdstip van het delict aanwezig was bij het huis van het slachtoffer.	

Digitaal	Analoog
Geluidsopname op de smartphone van de buurvrouw ten tijde van het toebrengen van het letsel aan Eva.	Verklaring arts over het toebrengen van het letsel van Eva.
Hieruit blijkt dat geschreeuw van Eva te horen is, een doffe klap en voorwerpen die op de grond vallen.	Hieruit blijkt dat de kaak van Eva gebroken is. De arts acht de kans groot dat een hard voorwerp dit letsel heeft veroorzaakt.
Het is aannemelijk dat de kaak gebroken is door toedoen van iemand anders.	

Digitaal	Analoog
Verzoek tot monitoren van het Instagramaccount van verdachte Tony.	Verzoek tot observatie van verdachte Tony.
Officier van justitie wijst de vordering af.	

Digitaal	Analoog
Inzien van de loggegevens van de bank-app van Henk Elands.	Resultaten van een verhoor van Henk Elands.
De vordering tot het inzien van de loggegevens wordt afgewezen.	Henk Elands beroept zich op zijn zwijgrecht.
Hieruit kunnen geen conclusies worden getrokken.	

Digitaal	Analoog
Een vriend van Tony geeft aan dat hij op zijn telefoon belastende berichten over het delict heeft ontvangen van Tony.	Een tweede slachtoffer van Tony meldt zich.
De vriend van Tony laat zien dat Tony een foto van de verwondingen van Eva heeft gedeeld en naar hem heeft geappt.	Het slachtoffer verklaart dat zij is bedreigd door Tony dat hij haar kaak zou breken als ze niet naaktfoto's van zichzelf zou delen.
Hieruit blijkt dat het steeds aannemelijker wordt dat Tony Eva heeft mishandeld en hij degene is die haar kaak heeft gebroken.	

Digitaal	Analoog
Data afkomstig uit de uitgelezen telefoon van verdachte Tony met 18 GB aan data.	Dertig dozen met de administratie van verdachte Tony.
Door de overmatige hoeveelheid informatie en beperkte tijd geeft de coördinator van het onderzoek aan dat het niet mogelijk is om alles door te nemen. Er kunnen vooralsnog geen conclusies worden getrokken.	

Digitaal	Analoog
Door verdachte aangeleverde screenshots van de loggegevens van een game met profielnaam 'Tonzone'.	Door verdachte aangeleverde getuige.
Uit de screenshots van de loggegevens blijkt dat hij aan het spelen was tijdens de vermeende mishandeling. Ook heeft 'Tonzone' diverse chatgesprekken gevoerd tijdens het spelen van de game.	Getuige verklaart dat hij bij de verdachte was ten tijde van de mishandeling.
Hieruit blijkt dat Tony een alibi heeft op het tijdstip van het delict.	

Digitaal	Analoog
Verkenning van relevante fora op het darkweb in combinatie met nickname 'Tonzone'.	TCI-aanvraag (Team Criminele Inlichtingen) over Tony.
Hier komen helaas geen relevante resultaten uit voort.	

Bijlage 3. Oproep deelname casusonderzoek

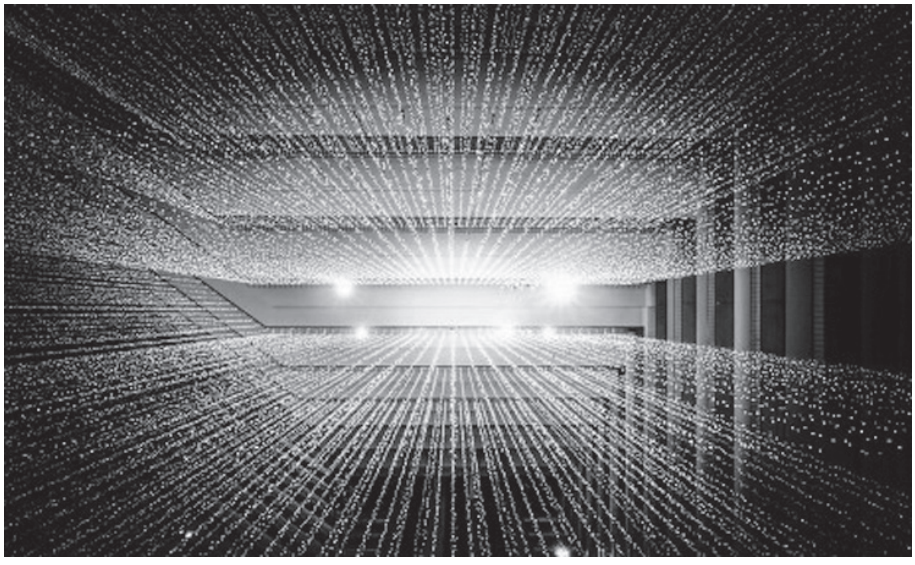
In samenwerking met NHL Stenden Hogeschool en de Politieacademie wordt binnen onze eenheid onderzoek gedaan naar opsporingswerk en hoe kansen daarbinnen beter kunnen worden benut. Dit onderzoek zal in april en mei plaatsvinden en duurt per persoon een klein uur. Het onderzoek houdt in dat collega's actief zelf aan de slag gaan met een casus.
Opdrachtgever van dit onderzoek is Politie en Wetenschap. De resultaten uit het onderzoek worden landelijk verspreid en gebruikt om te investeren in opsporingsmogelijkheden. Deelname aan dit onderzoek vanuit de teams is erg belangrijk. Dit mogen alle collega's zijn die mogelijk op een pd komen waar digitale sporen te vinden zijn. Uiteraard worden onderzoeksresultaten anoniem verwerkt.

Aanmelden
Aanmelden kan door een voorkeur voor locatie/datum/tijd (elk heel uur kun je deelnemen) te mailen naar: […]. Er wordt vervolgens een bevestiging toegestuurd waarin duidelijk wordt aangegeven waar je wanneer moet zijn.
Apeldoorn 9.00 – 16.00: 23 april, 6 mei, 13 mei, 16 mei
Zutphen 9.00 – 16.00: 23 april, 6 mei, 13 mei, 16 mei

Op basis van de oproep op de vorige bladzijde is onderstaand bericht geplaatst op intranet bij de Eenheid Noord-Nederland (aanpassingen zijn gedaan op initiatief van de teamleider van Team Digitale Opsporing en de beheerder van de pagina):

Collega's gezocht voor onderzoek naar digitaal opsporen

Laatst gewijzigd: 03-04-2019 | 07:43
Bron: Linda Wieland, Team Digitale Opsporing DRR



In samenwerking met NHL Stenden Hogeschool en de Politieacademie wordt binnen onze eenheid onderzoek gedaan naar opsporingswerk en hoe kansen daarbinnen beter kunnen worden benut. Dit onderzoek zal in april plaatsvinden en duurt per persoon een klein uur. Het onderzoek houdt in dat collega's actief zelf aan de slag gaan met een casus in een praktijkruimte.

Digitaal bewijs

"Digitaal bewijs wordt misschien wel belangrijker dan DNA-bewijs". In de digitale wereld laten we steeds meer digitale voetafdrukken achter. Een zoekmachine raadplegen, een e-mail versturen, een foto maken, autorijden, simpelweg op straat lopen: al deze activiteiten creëren digitale gegevens en dus bewijsmateriaal.

Graag deelname vanuit de teams

Opdrachtgever van dit onderzoek is Politie en Wetenschap. De resultaten uit het onderzoek worden landelijk verspreid en gebruikt om te investeren in opsporingsmogelijkheden. Deelname aan dit onderzoek vanuit de teams is erg belangrijk. Dit mogen

alle collega's zijn die mogelijk op een pd komen waar digitale sporen te vinden zijn. Affiniteit op digitaal gebied is niet nodig. Uiteraard worden onderzoeksresultaten anoniem verwerkt.

Aanmelden
Als je klikt op de locaties hieronder zie je een rooster waarop per locatie beschikbare tijden (met een groen vlak) worden weergegeven. Aanmelden kan door een voorkeur voor locatie/datum/tijdblok te mailen naar [dit mailadres]. Er wordt vervolgens een bevestiging toegestuurd waarin duidelijk wordt aangegeven waar je wanneer moet zijn.

– Balkengracht 3, Assen
– Rademarkt 12, Groningen
– Sontweg 8, Groningen
– Holstmeerweg 3, Leeuwarden

Bijlage 4. Verantwoording werving respondenten

Districtsrecherche Twente. Een oproep om aan het onderzoek deel te nemen is binnen de Districtsrecherche Twente op 24 april 2019 naar de hele afdeling verstuurd. Dit is vooraf kortgesloten met de teamleider. De oproep is opgenomen in bijlage 3. In de tekst van deze oproep is bewust weggelaten dat het om 'het benutten van digitale sporen' gaat en daarnaast is ook de naam van de onderzoeksgroep 'cybersafety' bewust vermeden. Dit om te voorkomen dat met name respondenten met affiniteit voor digitaal zouden deelnemen aan het onderzoek. Het doel van het onderzoek is gecommuniceerd na afloop van het casusonderzoek.

Geïnteresseerden konden zich voor opgave melden bij ondergetekende (per e-mail of telefonisch), waarna een afspraak kon worden gemaakt, zo veel mogelijk op de eigen werkplek van de respondenten. Via deze weg hebben zich uiteindelijk drie personen aangemeld. De afname van het experiment vond verspreid over twee dagen plaats in het politiebureau te Hengelo. Op de tweede dag heeft nog één extra persoon deelgenomen, nadat deze persoon via een collega kennis had genomen van het onderzoek.

Districtsrecherche Noord- en Oost Gelderland. Eerst is contact gelegd met de teamchef van de Districtsrecherche Noord- en Oost Gelderland waarin het onderzoek werd toegelicht en gevraagd of er binnen deze afdeling proefpersonen konden worden gezocht. De teamchef verwees de onderzoekers naar de digitaal specialist, met wie vervolgens contact is opgenomen en via wie op 18 april 2019 een soortgelijke e-mailbericht als binnen de Districtsrecherche Twente (afdelingsbreed) is uitgegaan. In deze oproep hadden geïnteresseerden de mogelijkheid om zich op een van twee locaties in te schrijven, te weten het hoofdbureau te Apeldoorn en het politiebureau te Zutphen, al naar gelang de werkplek van de betrokken respondenten. Uiteindelijk hebben zich twee proefpersonen opgegeven voor de locatie te Apeldoorn, waarvan er één niet is verschenen. Op diezelfde dag hebben zich echter nog vijf personen aangemeld nadat zij hiertoe door de onderzoekster op de werkplek waren uitgenodigd. Uiteindelijk hebben zes personen deelgenomen aan het experiment, allen op het hoofdbureau te Apeldoorn.

Noord-Holland. Uit de Eenheid Noord-Holland is een aantal recherchekundigen in opleiding met opsporingservaring (tussen drie en vijf jaar in dienst) benaderd. Van deze groep zijn zes personen telefonisch en per e-mail benaderd door de onderzoeker met de vraag om deel te nemen aan het experiment. Uiteindelijk is met drie respondenten

een afspraak gemaakt voor deelname aan het experiment. Twee respondenten hebben deelgenomen aan het experiment op hun eigen werkplek op het politiebureau te Hoofddorp. De andere respondent heeft aan het experiment deelgenomen op de locatie van de Politieacademie te Apeldoorn.

Oost- en Midden-Nederland. Uit de eenheden Oost-Nederland en Midden-Nederland zijn eveneens een aantal recherchekundigen in opleiding benaderd. Er zijn ongeveer twintig recherchekundigen in opleiding persoonlijk benaderd. Een deel is op de Politieacademie face-to-face aangesproken en gevraagd of zij mee wilden doen aan het experiment, een deel is per e-mail benaderd en een deel telefonisch. Er hebben zich dertien geïnteresseerden aangemeld, waarvan er uiteindelijk tien daadwerkelijk aan het experiment hebben deelgenomen. Negen respondenten hebben in Apeldoorn (Politieacademie) deelgenomen aan het experiment en één respondent heeft op haar werkplek op het politiebureau te Zwolle deelgenomen aan het experiment.

Noord-Nederland. In samenwerking met Team Digitale Opsporing is een oproep op intranet geplaatst (zie bijlage 3) en is een e-mail verzonden met dezelfde tekst als de oproep naar 27 teamchefs en/of vervangende teamchefs binnen de eenheid Noord-Nederland. Hoewel een tekst is voorgesteld voor de oproep en de instructie is gegeven om geen vermelding te maken van 'digitale sporen' dan wel 'cybersafety', zijn er toch enkele zinnen toegevoegd waarin wordt gesproken van digitale sporen (zie bijlage 3). Dit heeft mogelijk tot gevolg gehad dat in verhouding meer respondenten hebben deelgenomen die affiniteit hebben met het gebruik van digitale sporen.

Er is niet vastgesteld welke van de (vervangende) teamchefs deze e-mail daadwerkelijk binnen hun team hebben verspreid. Op een later moment is een reminder verstuurd naar de teamchefs én is de oproep naar de teamchefs gegaan van generieke opsporing, thematische opsporing en specialistische ondersteuning.

In overleg met vertegenwoordigers van de Eenheid Noord-Nederland is besloten het onderzoek af te nemen op vier locaties: Leeuwarden, Assen en Groningen (twee locaties). Uiteindelijk is het onderzoek verspreid over zeventien dagen afgenomen.

In Leeuwarden hebben negentien mensen zich aangemeld, in Assen 28 mensen en in Groningen zestien mensen (twaalf aan de Sontweg en vier aan de Rademarkt). Er zijn zeven respondenten die niet zijn komen opdagen of zich kort voor deelname hebben moeten afmelden voor het onderzoek in verband met spoedklussen.

Uiteindelijk hebben 76 respondenten deelgenomen aan het casusonderzoek: drie uit Eenheid Noord-Holland, zeventien uit de eenheden Oost- en Midden-Nederland en 56 uit Eenheid Noord-Nederland. Het casusonderzoek vond plaats tussen 4 april 2019 en 17 mei 2019.

Bijlage 5. **Details respondenten**

Werkzaamheden	Aantal
Tactisch rechercheur bij de districtsrecherche	20
Politiemedewerker in uniformdienst (Blauw)	14
Tactisch rechercheur bij de basisteamrecherche	12
Tactisch rechercheur bij de Regionale Recherche	11
Aspirant recherchekundige	6
Medewerker Intelligence	3
Zedenrechercheur	2
Administratief rechercheur Districtsrecherche	1
Coördinator rechercheur/recherchekundige	1
Digitaal specialist bij de Regionale Recherche	1
Financieel rechercheur bij de Districtsrecherche	1
Gedetacheerd bij het cybercrimeteam als tactisch rechercheur	1
Senior Intake en Service COP	1
Operationeel specialist digitaal bij Team Digitale Opsporing	1
Operationeel expert wijk thema	1

Functie	Aantal
Generalist	28
Operationeel specialist	16
Senior	14
Operationeel expert	9
Aspirant recherchekundige	6
Medewerker	2
Assistent B	1

Werkzaam bij de politie	Aantal
1-3 jaar	5
3-5 jaar	9
5-10 jaar	11
Langer dan 10 jaar	51

Opleiding of cursus op het gebied van digitale criminaliteit	Aantal
Geen	35
Zowel op het gebied van cybercrime als gedigitaliseerde criminaliteit	12
Alleen op het gebied van gedigitaliseerde criminaliteit	9
Alleen iRN	7
Alleen op het gebied van cybercrime	6
Open Source Intelligence	2
DCS-cursus	1
Digitale bewustwording	1
Enkele colleges gevolgd over cybercrime/digitaal	1
Aparte opleiding op het gebied van IT	1
Enkele themadagen gevolgd over cybercrime/digitaal	1

In het afgelopen jaar te maken gehad met zaken op het gebied van digitale criminaliteit	Aantal
Uitsluitend met dergelijke zaken te maken gehad	6
Veel mee te maken gehad	25
Niet veel, maar ook niet weinig mee te maken gehad	16
Weinig mee te maken gehad	29
Nooit mee te maken gehad	0

Bijlage 6. **Vragenlijsten**

Benutten digitale sporen

Ga eerst naar de receptie en geef instructies waar het onderzoek is, in geval respondenten niet weten waar ze naartoe moeten. Ze hebben allemaal een mail gekregen met de exacte ruimte. Bij de Sontweg is er geen receptie, dus daar mensen opvangen bij de ingang en ervoor zorgen dat de poort voor ze wordt opengedaan (gebruik je pasje).

Vraag bij de receptie waar je de poster mag ophangen (zie Sharepoint) voor het onderzoek. Dan kunnen er ook nog 'binnenlopers' langskomen.

Leg klaar: opnameapparaat, casus en twee stapels met de keuzes.
Zorg ervoor: dat de laptop voldoende batterij heeft.

Let op: NOEM NIETS OVER DIGITAAL DAN WEL ANALOOG. Spreek alleen over 'bewijsstukken'.

Respondentnummer (zie Sharepoint)
……

Observator
☐ Elske Posthuma
☐ Renske Zuurveen
☐ Jan Aink
☐ Mirjam Uenk
☐ Willem Bantema

Datum
MM DD JJJJ

Locatie
☐ Eenheid Noord-Nederland
☐ Eenheid Oost-Nederland
☐ Anders:

Casus
Stappenplan:
1. Laat de respondent de casus lezen.
2. Leg uit: "Het is straks de bedoeling dat je steeds een keuze maakt tussen twee bewijsstukken. Kies het bewijsstuk waar jijzelf met betrekking tot het oplossen van deze casus bij voorkeur voor zou kiezen. Normaal gesproken zou je wellicht beide bewijsstukken kiezen, maar wij willen dat je een keuze maakt tussen één van de twee".
3. Leg steeds de twee keuzes voor.
4. Respondent maakt een keuze (leg keuze vast: zowel in deze vragenlijst als op het keuzeblad).
5. Stel drie vragen (leg de antwoorden vast)
6. NA DE DRIE VRAGEN: toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
7. Klik op 'volgende' en volg het stappenplan opnieuw. Er zijn 10 keuzes.

Vraag eventueel (zo nodig) aan de respondent of je ten behoeve van het onderzoek het gesprek mag opnemen. Dat de opname na verwerking direct wordt verwijderd (probeer dezelfde dag nog de gegeven antwoorden te verwerken).

(1) Welke keuze wordt gemaakt?
☐ Analyse van de contacten van Eva op Instagram en Facebook
☐ Resultaten buurtonderzoek in omgeving plaats delict

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
…….

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…….

Casus
Stappenplan:
1. Leg de twee keuzes voor.
2. Respondent maakt een keuze (leg keuze vast).
3. Stel de drie vragen (leg antwoorden vast).
4. Toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
5. Klik op 'volgende'.

(2) Welke keuze wordt gemaakt?
☐ Verhoor van Roy (vriend van verdachte Tony)
☐ Open bronnenonderzoek op nickname 'Tonzone'

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
…….

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…….

Casus
Stappenplan:
1. Leg de twee keuzes voor.
2. Respondent maakt een keuze (leg keuze vast).
3. Stel de drie vragen (leg antwoorden vast).
4. Toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
5. Klik op 'volgende'.

(3) Welke keuze wordt gemaakt?
☐ Getuigenverklaring van overbuurman van Eva
☐ Modem en router uitlezen van Eva

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
……..

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…….

Casus
Stappenplan:
1. Leg de twee keuzes voor.
2. Respondent maakt een keuze (leg keuze vast).

3. Stel de drie vragen (leg antwoorden vast).
4. Toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
5. Klik op 'volgende'.

(4) Welke keuze wordt gemaakt?
☐ Geluidsopname die de buurvrouw met haar smartphone heeft gemaakt
☐ Verklaring arts over het letsel van Eva

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
…….

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…….

Casus
Stappenplan:
1. Leg de twee keuzes voor.
2. Respondent maakt een keuze (leg keuze vast).
3. Stel de drie vragen (leg antwoorden vast).
4. Toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
5. Klik op 'volgende'.

(5) Welke keuze wordt gemaakt?
☐ Verzoek tot observatie van verdachte Tony
☐ Verzoek tot monitoren Instagram account van verdachte Tony

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
…….

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…….

Casus
Stappenplan:
1. Leg de twee keuzes voor.
2. Respondent maakt een keuze (leg keuze vast).
3. Stel de drie vragen (leg antwoorden vast).
4. Toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
5. Klik op 'volgende'.

(6) Welke keuze wordt gemaakt?
☐ Inzien van loggegevens app internetbankieren van Henk Elands
☐ Resultaten van verhoor van Henk Elands

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
…….

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…….

Casus
Stappenplan:
1. Leg de twee keuzes voor.
2. Respondent maakt een keuze (leg keuze vast).
3. Stel de drie vragen (leg antwoorden vast).
4. Toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
5. Klik op 'volgende'.

(7) Welke keuze wordt gemaakt?
☐ Een tweede slachtoffer van Tony meldt zich
☐ Belastende berichten over Tony op telefoon van vriend van Tony

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
…….

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…

Casus
Stappenplan:
1. Leg de twee keuzes voor.
2. Respondent maakt een keuze (leg keuze vast).
3. Stel de drie vragen (leg antwoorden vast).
4. Toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
5. Klik op 'volgende'.

(8) Welke keuze wordt gemaakt?
☐ 18 GB data afkomstig uit uitgelezen telefoon van verdachte Tony
☐ Dertig dozen met administratie van verdachte Tony

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
…….

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…….

Casus
Stappenplan:
1. Leg de twee keuzes voor.
2. Respondent maakt een keuze (leg keuze vast).
3. Stel de drie vragen (leg antwoorden vast).
4. Toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
5. Klik op 'volgende'.

(9) Welke keuze wordt gemaakt?
☐ Door verdachte aangeleverde getuige
☐ Door verdachte aangeleverde screenshots van game

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
…….

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…….

Casus
Stappenplan:
1. Leg de twee keuzes voor.
2. Respondent maakt een keuze (leg keuze vast).
3. Stel de drie vragen (leg antwoorden vast).
4. Toon conclusie van het bewijsstuk: wat blijkt uit het bewijsstuk (respondent mag bladzijde(n) omslaan)
5. Klik op 'volgende'.

(10) Welke keuze wordt gemaakt?
☐ Verkenning dark web op nickname 'Tonzone'
☐ TCI aanvraag

Vraag 1: Waarom heb je voor bewijsstuk X gekozen?
…….

Vraag 2: Waarom heb je bewijsstuk Y NIET gekozen?
…….

Vraag 3: Hoe zou je normaal gesproken met dit bewijsstuk (dat je hebt gekozen) aan de slag gaan? (gelet op de casus)
…….

Nagesprek
Afsluiting
Kun je een algemene toelichting geven op de door jou gemaakte keuzes?
…….

Heeft het resultaat van ieder bewijsstuk invloed gehad op jouw daaropvolgende keuze?
…….

Wil je verder nog iets toelichten over jouw ervaringen met het gebruik van digitale sporen?
…….

Vragenlijst
Deze vragenlijst bestaat uit zes korte vraagblokken. U kunt per vraag meestal één antwoord kiezen. Wanneer u meerdere antwoorden kunt kiezen, wordt dit vermeld en zijn de vakjes voor de antwoordmogelijkheden niet rond, maar vierkant.

Er zijn geen goede of slechte antwoorden. Kies zorgvuldig het antwoord dat bij u past. Uw antwoorden worden anoniem verwerkt.

Algemene vragen
Wat typeert uw huidige werkzaamheden het best? *
☐ Ik ben politiemedewerker in uniformdienst (Blauw)
☐ Ik ben tactisch rechercheur bij de basisteamrecherche (VVC teams, etc.)
☐ Ik ben tactisch rechercheur bij de districtsrecherche
☐ Ik ben tactische rechercheur bij de regionale recherche
☐ Anders:

Wat is uw functie? *
☐ Assistent A
☐ Assistent B
☐ Medewerker
☐ Generalist
☐ Senior
☐ Operationeel expert
☐ Operationeel specialist
☐ Anders:

Hoe lang bent u werkzaam bij de politie? *
☐ 0-1 jaar
☐ 1-3 jaar
☐ 3-5 jaar
☐ 5-10 jaar
☐ Langer dan 10 jaar

Wat is uw geboortejaar? (vier cijfers)
…….

Wat is uw geslacht? *
☐ Man
☐ Vrouw

Hebt u een opleiding of cursus gevolgd op het gebied van digitale criminaliteit? (meerdere antwoorden mogelijk) *
☐ Ja, zowel op het gebied van cybercrime als gedigitaliseerde criminaliteit

☐ Ja, alleen op het gebied van cybercrime
☐ Ja, alleen op het gebied van gedigitaliseerde criminaliteit
☐ Ja, maar onbekend of het ging over cybercrime of gedigitaliseerde criminaliteit
☐ Ja, ik heb een aparte opleiding gevolgd op het gebied van IT
☐ Ja, een cursus gericht op iRN
☐ Nee
☐ Anders:

Hoeveel opleidings- en/of cursusdagen heeft u (ongeveer) gevolgd op het gebied van digitale criminaliteit? *
…….

In hoeverre hebt u het afgelopen jaar te maken gehad met zaken op het gebied van digitale criminaliteit? *
☐ Uitsluitend met dergelijke zaken te maken gehad
☐ Veel mee te maken gehad
☐ Niet veel, maar ook niet weinig mee te maken gehad
☐ Weinig mee te maken gehad
☐ Nooit mee te maken gehad

Geef aan in hoeverre u het eens bent met onderstaande stellingen *

	Helemaal mee oneens	Enigszins mee oneens	Niet mee oneens, niet mee eens	Enigszins mee eens	Helemaal mee eens
Ik weet welke digitale sporen van belang zijn voor opsporingsonderzoek					
Ik weet hoe de 7 W's (wie, wat, waar, waarmee, welke wijze, wanneer, waarom) kunnen worden toegepast om de relevantie van digitale sporen te bepalen					
Ik ken mijn eigen beperking(en) bij het verrichten van een opsporingsonderzoek naar digitale criminaliteit					
Ik weet hoe ik moet handelen wanneer ik bij het verrichten van opsporingsonderzoek naar digitale criminaliteit onvoldoende kennis heb					
Ik weet wat 'vluchtige gegevens' zijn					

	Helemaal mee oneens	Enigszins mee oneens	Niet mee oneens, niet mee eens	Enigszins mee eens	Helemaal mee eens
Ik ken de bevoegdheden tot inbeslagname van gegevensdragers					
Ik weet welke gegevensdragers op een PD relevant zijn voor inbeslagname					
Ik weet welke gegevensdragers kunnen worden uitgelezen					
Ik weet tijdens een onderzoek wanneer het nuttig/noodzakelijk is om gegevensdragers uit te lezen					
Ik weet hoe ik softwarepakketten moet gebruiken om digitale sporen te analyseren					
Ik weet hoe ik de bevindingen van digitaal sporenonderzoek moet vastleggen (dossiervorming)					

	Helemaal mee oneens	Enigszins mee oneens	Niet mee oneens, niet mee eens	Enigszins mee eens	Helemaal mee eens
Ik weet welk type informatie je kunt vinden op welk type internet bron					
Ik weet waar ik op internet moet zoeken om persoonsgegevens te achterhalen					
Ik weet waar ik op internet moet zoeken om bedrijfsgegevens te achterhalen					
Ik weet hoe ik als politiemedewerker zo weinig mogelijk sporen kan achterlaten bij het zoeken op internet					

Er volgen een aantal vragen over het gebruik van digitale sporen. Iedere vraag in onderstaande tabel gaat over: De komende maand digitale sporen gebruiken om aan een zaak te werken. Geef het antwoord dat het meeste met uw mening overeenkomt.

Ik ben van plan de komende maand digitale sporen te gebruiken om aan een zaak te werken

	1	2	3	4	5	6	7	
Helemaal mee oneens	☐	☐	☐	☐	☐	☐	☐	Helemaal mee eens

Als ik de komende maand digitale sporen gebruik om aan een zaak te werken, dan vind ik dat

	1	2	3	4	5	6	7	
Helemaal mee oneens	☐	☐	☐	☐	☐	☐	☐	Helemaal mee eens

De meeste collega's die ik respecteer gebruiken de komende maand digitale sporen om aan een zaak te werken

	1	2	3	4	5	6	7	
Helemaal mee oneens	☐	☐	☐	☐	☐	☐	☐	Helemaal mee eens

Als ik de komende maand digitale sporen gebruik om aan een zaak te werken, dan vind ik dat

	1	2	3	4	5	6	7	
Vevrvelend	☐	☐	☐	☐	☐	☐	☐	Prettig

Ik ben er zeker van dat ik in staat ben de komende maand digitale sporen te gebruiken om aan een zaak te werken, als ik dat wil

	1	2	3	4	5	6	7	
Helemaal mee oneens	☐	☐	☐	☐	☐	☐	☐	Helemaal mee eens

De meeste collega's wiens mening ik waardeer, keuren het goed wanneer ik de komende maand digitale sporen gebruik om aan een zaak te werken

	1	2	3	4	5	6	7	
Zeer onwaarschijnlijk	☐	☐	☐	☐	☐	☐	☐	Zeer waarschijnlijk

Of ik de komende maand digitale sporen ga gebruiken om aan een zaak te werken, ligt volledig aan mijzelf

	1	2	3	4	5	6	7	
Helemaal mee oneens	☐	☐	☐	☐	☐	☐	☐	Helemaal mee eens

Als ik de komende maand digitale sporen gebruik om aan een zaak te werken, dan vind ik dat

	1	2	3	4	5	6	7	
Slecht	☐	☐	☐	☐	☐	☐	☐	Goed

De keuze om de komende maand digitale sporen te gebruiken om aan een zaak te werken, ligt

	1	2	3	4	5	6	7	
Buiten mijn controle	☐	☐	☐	☐	☐	☐	☐	Binnen mijn controle

Ik heb de intentie om de komende maand digitale sporen te gebruiken om aan een zaak te werken

	1	2	3	4	5	6	7	
Helemaal mee oneens	☐	☐	☐	☐	☐	☐	☐	Helemaal mee eens

De meeste collega's zoals ik, zullen de komende maand digitale sporen gebruiken om aan een zaak te werken

	1	2	3	4	5	6	7	
Helemaal mee oneens	☐	☐	☐	☐	☐	☐	☐	Helemaal mee eens

Ik verwacht dat ik de komende maand digitale sporen ga gebruiken om aan een zaak te werken

	1	2	3	4	5	6	7	
Helemaal mee oneens	☐	☐	☐	☐	☐	☐	☐	Helemaal mee eens

De meeste collega's die belangrijk voor mij zijn, vinden dat ik de komende maand digitale sporen moet gebruiken om aan een zaak te werken

	1	2	3	4	5	6	7	
Helemaal mee oneens	☐	☐	☐	☐	☐	☐	☐	Helemaal mee eens

De komende maand digitale sporen gebruiken om aan een zaak te werken is

	1	2	3	4	5	6	7	
Moeilijk	☐	☐	☐	☐	☐	☐	☐	Makkelijk

Als ik de komende maand digitale sporen gebruik om aan een zaak te werken, dan vind ik dat

	1	2	3	4	5	6	7	
Belemmerend	☐	☐	☐	☐	☐	☐	☐	Bevorderlijk

Stel dat u de komende maand aan 10 zaken werkt. In hoeveel van die zaken verwacht u gebruik te maken van digitale sporen?

1	2	3	4	5	6	7	8	9	10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

In hoeverre bent u het eens met onderstaande stellingen?

	Helemaal mee oneens	Enigszins mee oneens	Niet mee oneens, niet mee eens	Enigszins mee eens	Helemaal mee eens
Ik weet hoe ik met digitale sporen moet werken					
Ik ben onbekend met de mogelijkheden die digitale sporen bieden					
Ik zie de potentie van digitale sporen					
Er zijn voldoende faciliteiten om met digitale sporen te werken					
Ik ben bang om fouten te maken met digitale sporen					
Werken met digitale sporen is gebruiksvriendelijk					
Digitale experts zijn te druk om mij te helpen met het werken met digitale sporen					
Ik ben onbekend met de bevoegdheden die ik nodig heb om met digitale sporen te werken					

Er is voldoende jurisprudentie om met digitale sporen te werken
Data uit digitale gege-vensdragers zijn omvangrijk om mee te werken
Er is onvoldoende capaciteit om met digitale sporen te werken
Digitale sporen zijn betrouwbaar
Ik heb interesse in het gebruik van digitale sporen
Ik ben onzeker over mijn kennis over digitale sporen
Werken met digitale sporen brengt ongewenste veranderin-gen in politiewerk met zich mee

Dit is het einde van de vragenlijst. Ten behoeve van het onderzoek willen we u over twee weken een tweede vragenlijst voorleggen die maximaal drie minuten van uw tijd zal vragen. U zou ons enorm helpen als u deze vragenlijst wilt invullen. Uiteraard worden uw antwoorden ook dan anoniem opgeslagen. Indien u hieraan wilt meewerken, kunt u hieronder uw e-mailadres invullen.

Jouw antwoord

…….

Bijlage 7. Toelichtingen op handelingsstrategieën digitale bewijsstukken

Nadat een keuze werd gemaakt voor een digitaal bewijsstuk, is gevraagd hoe de opsporingsmedewerkers normaal gesproken met dit bewijsstuk aan de slag zouden gaan. In onderstaande tabellen worden achtereenvolgens de toelichtingen genoemd per keuze. De formulering van de antwoorden is ten behoeve van de leesbaarheid hier en daar aangepast.

Keuze 1: Handelingsstrategie raadplegen social media

Bevriezen van gegevens. Vorderen dat account afgesloten wordt. Daarna inhoud vorderen.
Een BOB-aanvraag doen via het KLPD.[34]
Gerichte vragen formuleren voor het opsporingsonderzoek en de telefoon afleveren bij het digitale team voor vordering en analyse.
Inloggen en screenshots maken van interessante bevindingen. Zo mogelijk met iRN.
Kijken naar de inloggegevens en welke IP-adressen daaraan gekoppeld zijn, kijken naar foto's, contacten, hoe vaak geliked, geolocatie,[35] posts, reacties, etc.
Met hulp van de officier van justitie een vordering opmaken om de gegevens te krijgen van Instagram en Facebook.
Onmiddellijk een tap op aangeefster Eva haar telefoon en een social media-scan uitvoeren.
Overleggen met officier van justitie over eventuele stelselmatigheid.
Telefoon in beslag nemen en bij team 'digi' brengen voor veiligstellen en uitlezen.
Toestemming vragen aan [aangeefster Eva] om dit in te zien.
Via de speciale afdelingen die daarvoor bedoeld zijn (crimeteam, afdeling 'digi', Open Source Intelligence, internetrechercheur, Dienst Regionale Informatie Organisatie, specialisten social media).
Via een iRN-computer op het account kijken.
Zelf zoeken.

34 Het Korps Landelijke Politiediensten (KLPD) bestond van 1993 tot 2013 en was belast met taken die de grenzen van de regiokorpsen overschreden dan wel een landelijk of internationaal belang hadden. Het KLPD is op 1 januari 2013 opgegaan in de Nationale Politie. https://thesaurus.politieacademie.nl/Thesaurus/Term/2272, geraadpleegd 18 november 2019). De politie kent nu een Landelijke Eenheid (LE).

35 Geolocatie verwijst naar identificatie van de geografische locatie van een apparaat.

Keuze 2: Handelingsstrategie open bronnenonderzoek

Alles wat relevant is bij het zoeken op de nickname onderzoeken (wat doet hij, wat doen zijn vrienden, relaties, gesprekken, etc.).
BOB-melding om onderzoek te kunnen doen.
Digitaal platform bellen en samen kijken.
Een collega vragen met specialistische kennis (Open Source Intelligence, iRN, digitaal rechercheur, etc.).
Uitzetten bij Dienst Regionale Informatie Organisatie.
Vastleggen via een p.v. hoe is gezocht en wat het resultaat daarvan is.
Via Open Source Intelligence.
Zo nodig toestemming vragen van officier van justitie.
Zoeken met behulp van een iRN-computer.
Zoekmachines gebruiken en zoeken op [de nickname van verdachte Tony].
Zoekvragen opstellen voor de specialisten digitaal.

Keuze 3: Handelingsstrategieën uitlezen modem en router

Bij voorkeur ter plekke onderzoeken, zodat het verlies van gegevens wordt voorkomen.
Collega's moeten de WiFi uitzetten, zodat gegevens niet overschreven worden.
Foto's maken van locatie modem/router thuis.
IP-adressen verzamelen die verbinding hebben gemaakt met de router.
Meenemen, veiligstellen en aan collega's van Team Digitale Opsporing overdragen.
Met digitaal experts overleggen.
Team Digitale Opsporing raadplegen. Zij lezen de modem/router uit en maken daar p.v. van.
Uitzetten bij digitaal platform.

Keuze 4: Handelingsstrategieën geluidsopname smartphone

Als het na beluisteren niet relevant blijkt te zijn, dan een uittreksel maken in een p.v..
Digitale expertise bellen en vragen om advies.
Door middel van een vordering opvragen.
Eigenaresse van de smartphone kan het bestand via e-mail of Whatsapp toesturen.
Eigenaresse van smartphone het bestand laten opsturen of op USB[-stick] laten zetten.
Expert bevragen over de echtheid van het geluidsbestand.
Geluidsbestand in het programma Elvis[36] zetten.
Geluidsopname innemen en het bestand woordelijk uitwerken. Het uitgewerkte bestand komt in het dossier.
Het geluidsbestand laten beluisteren door een tapper.
Met een harddisk van de afdeling naar de eigenaresse gaan en het bestand erop zetten.
Telefoon formeel in beslag nemen, naar afdeling 'digi' brengen en laten uitlezen.

36 Elvis is een softwareprogramma waarmee burgers zelf documenten/foto's/filmpjes voor de opsporing kunnen uploaden.

Telefoon laten uitlezen en in de metadata kijken wanneer de geluidsopname gemaakt is.
Van seconde tot seconde rapporteren in een p.v.
Vragen of de eigenaresse van de smartphone op het bureau langs wil komen. Als zij het afspeelt, de opname overnemen.
Vrijwillig laten afstaan door de eigenaresse van de smartphone.

Keuze 5: Handelingsstrategieën monitoren Instagram

Afdeling 'digi' vragen om te monitoren.
Delegeren aan analisten.
Een specialist in het team benaderen.
Geen ervaring mee/weet niet.
Instagram af en toe zelf in de gaten houden.
Rechtshulpverzoek indienen voor Instagram.
Script maken, zodat veranderingen in het account worden doorgegeven (na toestemming stelselmatigheid).
Uitzetten bij Dienst Regionale Informatie Organisatie of OSINT.
Via het webcare team[37].
Via iRN zelf onderzoeken.
Vordering via officier van justitie of rechter-commissaris (stelselmatige observatie).
Webcrawler[38] op zetten via afdeling digitaal.

Keuze 6: Handelingsstrategieën loggegevens bank-app

Advies vragen bij een financieel expert uit het team.
Geen ervaring met dit bewijsstuk.
Laten uitlezen door afdeling digitaal.
Loggegevens gebruiken om te kijken vanaf welk IP-adres is ingelogd, met welk apparaat, naar welke rekeningen is overgemaakt, vanaf welke locatie, contante opnames van geld, etc.
Opvragen met een vordering. Toestemming van officier van justitie nodig.
Team digitale recherche laten aanvragen en doorzetten.
Telefoon in beslag nemen en uitlezen.
Via het crimeteam.
Vorderen bij de bank.

Keuze 7: Handelingsstrategieën berichten op smartphone

Advies inwinnen over hoe hiermee om te gaan.
Eerst getuigenverklaring laten afleggen en dan berichten als bijlage bij p.v. toevoegen.

37 Politieteam waar burgers via social mediakanalen tips, meldingen en vragen kunnen achterlaten. Zie https://www.politie.nl/nieuws/2018/oktober/3/snel-en-gemakkelijk-contact-met-politie-via-social-media.html, geraadpleegd 18 oktober 2019.

38 Een softwareprogramma dat internetpagina's doorzoekt naar bepaalde gegevens en die vastlegt.

Getuigenverklaring opnemen.
Indien getuige vrijwillig telefoon afstaat, kan telefoon worden ingenomen en kopie worden gemaakt.
Met digital experts kijken wat erop staat en in gesprek gaan.
Screenshot maken en lezen en verwoorden in p.v..
Telefoon in beslag nemen met toestemming van officier van justitie.
Telefoon uitlezen en als dat niet (helemaal) hoeft, dan een kleiner gedeelte of een foto/schermafdruk maken.
Veilig laten stellen door Team Digitale Opsporing. Zij leveren een rapportage.
Whatsappberichten laten doorsturen via Whatsapp of e-mail.

Keuze 8: Handelingsstrategieën data smartphone[39]

Concrete onderzoeksvragen formuleren voor de experts die de telefoon uitlezen.
Data raadplegen op harde schijf of CD-ROM.
Door digitaal experts onderzoek laten doen.
Filteren van informatie. Zoeken op trefwoorden.
Forensische software inzetten (bijvoorbeeld UFED of XRY[39]).
Nog geen ervaring met telefoons (laten) uitlezen.
Selectief zoeken op datgene wat interessant is voor een zaak. In dit geval foto's, social media, chat en internetbankieren.
Telefoon in beslag nemen via toestemming van officier van justitie, experts lezen telefoon uit (kopie) en maken een rapportage. In de rapportage zelf zoeken naar relevante informatie.
Telefoon uitlezen kan ik zelf.

Keuze 9: Handelingsstrategieën screenshots game

Aan digitaal experts geven en vragen wanneer deze screenshots zijn gemaakt.
Digitaal experts vragen wat er uitgezocht kan worden en of het gemanipuleerd is.
Gegevens vorderen bij de game om te kijken of de screenshots overeenkomen met de werkelijke loggegevens.
In zorgvuldig overleg met officier van justitie over vordering tot inloggen bij de game.
Kijken naar de EXIF-data van de screenshots.
Laten uitlezen door software-expert.
P.v. van bevindingen maken.
Besluit van rechter-commissaris nodig.
Screenshots onderzoeken op echtheid.
Screenshots printen en bevindingen opnemen in een beeld-p.v.
Taalgebruik en overige kenmerkende eigenschappen in de game gebruiken om te controleren of het echt de verdachte was.
Tactische aanwijzingen uit dit bewijsstuk gebruiken in het verhoor.

39 UFED (Universal Forensic Extraction Device) en XRY (vgl. X-ray) zijn softwareprogramma's voor (forensisch) onderzoek aan mobiele telefoons.

Keuze 10: Handelingsstrategieën onderzoek dark web[40]

Cyberrechercheur pakt het op.
Een expert van de afdeling cybercrime, Dienst Regionale Informatie Organisatie, Team Digitale Opsporing of Landelijke Eenheid raadplegen en inzetten.
Geen ervaring/weet niet.
IRN-computer gebruiken en zelf kijken.
THTC inschakelen.
Via het Open Source Intelligence-framework.
Via VPN[40] op het darkweb zelf kijken.
Vordering opstellen.

40 Virtual Private Network, bedoeld om met encryptie beveiligd en met verhuld IP-adres verbinding met het internet te maken.

Bijlage 8. Antwoorden op de open vraag: 'Wilt u verder nog iets toelichten over uw ervaringen met het gebruik van digitale sporen?'

De open vraag 'Wilt u verder nog iets toelichten over uw ervaringen met het gebruik van digitale sporen?' is door respondenten op verschillende manieren geïnterpreteerd en beantwoord. Het gros heeft een antwoord gegeven dat ingaat op persoonlijke ervaringen met digitale sporen (N=52). Daarom zijn de gegeven antwoorden die hierop gericht waren eerst geclusterd in hoeveelheid ervaring (weinig, enigszins, veel). Sommige citaten zijn opgeknipt en in meerdere boxen opgenomen.

Antwoorden door respondenten met weinig ervaring met digitale sporen (N=22)

Daar ben ik niet op ingericht. We komen wel veel digitale sporen tegen.
Dat is niet zo heel veel. Tuurlijk de laatste tijd bij zeden met al die foto's, steeds meer. Je probeert wel heel veel dingen te doen. Het heeft mijn interesse niet, vandaar dat ik het niet snel doe.
Deze is minimaal. In het verleden heb ik vaak team Digitale Opsporing gevraagd om te helpen. Veilig stellen en uitlezen heb ik wel eens geleerd, maar dat is alweer te lang geleden.
Er zijn heel veel dingen waar ik geen idee van heb. Ik weet wel waar ik mij tot moet richten.
Geen ervaring. Ik heb vier weken terug iemand gehad die aangifte wilde doen van hacken. Ik zei: ik moet wat hebben voor een vervolgonderzoek, dus je moet eerst naar de fraude afdeling. Zo kan ik er niets mee.
Heel weinig ervaring.
Het is niet mijn expertise. Ik doe wel eens wat open source, maar verder niet.
Het is niet mijn hobby om achter een computer te zitten. […] Doordat je toch niet bent opgevoed met computers. Ik heb er geen belang bij.
Ik heb daar nog niet veel ervaring mee gehad in de praktijk.
Ik heb niet heel erg veel digitale onderzoeken gedraaid.
Ik heb te weinig ervaring met digitale sporen.
Ik heb wel eens telefoon laten uitlezen, maar dat bleek later niet nodig te zijn.
Ik heb weleens een telefoon laten uitlezen en bankgegevens, verder dan dat ben ik nog niet gekomen. Met de telefoon heeft wel echt de toekomst, als je kijkt naar jeugd is de telefoon hun leven
Laat ik aan collega's over, dan krijg je de juiste informatie. Niet zelf mee knoeien en dan de helft missen.
Minimaal. Sinds een paar weken met UFED bezig.
Niet zoveel ervaring mee. Ik vind dat er mensen gespecialiseerd in moeten zijn, die moeten dat doen. Tegenwoordig gaat er ook een digi mee met zoekingen bijvoorbeeld.

Nog niet zoveel ervaring. Ik ben nu 3 jaar werkzaam en ik heb 1x een mobiel uitgeplozen.
Omdat ik er minder ervaring mee heb, stel ik de vraag altijd wel aan digi, waarbij ik de casus voorleg, en vraag of er nog digitale mogelijkheden zijn.
Wat ik vervelend vind voor mijzelf is dat het best wel weg is gezakt. Ik merk dat ik soms zoiets heb van hoe ging dat ook alweer.
Weinig ervaring. Ik vind het niet zo interessant, ik weet wel dat het belangrijk is en de toekomst is.
Weinig ervaring. Wel met camerabeelden. Open bronnenonderzoek doe ik wel, maar verder dan dat niet.
Zeer weinig. Ik weet niet wat er allemaal mogelijk is.

Antwoorden door respondenten die enigszins ervaring hebben met digitale sporen (N=22)

Als de mogelijkheid er is, dan doen we dat. We merken vaak bij inbraken dat we veel gebruik maken van digitale sporen zoals video-opnames, beveiligingscamera's, opnames en foto's op telefoons.
Bankgegevens weet ik door een aantal keren gedaan te hebben zijn best wel flinke daderindicaties in kaart gebracht. Dat vind ik het mooie aan digitale sporen.
Bij zeden hebben we veel met telefoons te maken waar rotzooi op staat. Ik zit geregeld bij digi en Team Bestrijding Kinderporno Kindersekstoerisme (TBKK) om te laten lezen en bekijken.
Ik ben bij ons wel degene die veel met digitale sporen en cybercrime doet. Ik denk dat het soms ook wel is van in het land der blinden. Ik gebruik wel social media om ernaar te kijken voordat ik iemand uitnodig voor verhoor. Het dark web check ik ook wel eens. Verder houd ik mij bezig met het uitlezen van telefoons.
Ik doe administratief werk, maar ik heb wel een digitale achtergrond. Veel data veiliggesteld en geanalyseerd.
Ik heb tijdje bij milieu gezeten, daar veel gedaan met telefoons.
Ik heb vooral ervaring met onderzoek aan telefoons en social media scans, dus kijken welke contacten iemand heeft. Op de afdeling is een fakeaccount op een iRN computer. Ik heb aan de hand daarvan contacten aangetoond en bijvoorbeeld om foto's te vergelijken met camerabeelden, dus met als doel om iemand te identificeren.
Ik heb weleens een telefoon laten uitlezen en bankgegevens opgevraagd, verder dan dat ben ik nog niet gekomen.
Ik heb zelf opleiding UCO gedaan (uitlezen telefoon). Ik ga me bezig houden met cybercrime.
Ik weet er iets van, maar ben zeker geen specialist. Ik vind dat de toekomst daar heel erg ligt. Ik vind niet dat ik alles moet weten, maar ik vind het belangrijk om te kunnen signaleren en om te kunnen weten waar de kansen liggen om een specialist daarover te bevragen. Een specialist moet weten over de juridische implicaties en de praktische toepasbaarheid.
Ik werk nu een jaar bij het cybercrimeteam en ik leer elke dag. Er is een hele wereld voor me opengegaan. Ik ben nog steeds een digibeet. Ik ben heel blij met hoe ver ik ben. Niveau is absoluut gegroeid. Nu maak ik tapaanvragen en doe ik van alles.
In het dagelijks werk: af en toe personen opzoeken. Via Facebook bijvoorbeeld. Via Google, social media. Maar anders kom ik daar weinig mee in aanraking. iRN hebben we wel, maar doe ik niet heel veel mee. Ik doe het via mijn eigen account of zonder account opzoeken. Meer met personen.
Met Facebook regelmatig, wanneer mensen met nepaccounts aangifte doen. Dan zoek je op het IP-adres van die nepaccounts. Ik doe veel jeugdzaken. Er zijn continu pubers die niet leren en naaktfoto's in de omloop brengen. Die met wederzijdse toestemming gemaakt zijn, maar die later worden gedeeld uit rancune. Meisjes van 15/16 die in de gang hangen naakt, daar gaan ze kapot aan. Je moet naar de bron van de foto, als het zich in een kleine omgeving afspeelt vinden we de dader wel, maar vaak gaat het heel Nederland door. Je kunt er niks aan veranderen. Veel via Whatsapp.
Mijn ervaring bij onderzoek naar cybercrime is dat je veel onderzoek doet wat tot weinig leidt en waarbij je moeilijk tot een verdachte komt.
Mijn mindset gaat richting digitaal, maar ik laat het rechercheren over aan deskundigen, omdat ik een onderzoek niet wil verknoeien.
Onderzoeken van uitgelezen telefoons, althans in UFED werden telefoons uitgelezen. Ook gegevensdragers in beslag genomen bij doorzoekingen. De iRN computer heb ik ook geraadpleegd met fake accounts.

Open bronnen doe je wel snel en uitlezen telefoon komt ook veel voor.
Regelmatig komen er telefoons voorbij die uitgelezen zijn. Ik maak daar ook gebruik van. Net cursus voor uitlezen telefoons gevolgd.
Tot op zekere hoogte doe ik dit dagelijks. Ik werk wel met digitaal, maar ik ben er bekend mee, ik weet ongeveer wat ik kan opvragen en welke wegen ik moet bewandelen. Maar ik ben lerende. Binnen het team kan ik gemakkelijk experts vragen. Voor Districtsrecherche-collega's ook. Die hebben het digitaal platform. Ze kunnen ondersteuning vragen aan het digitaal platform.
We doen wel wat onderzoek ernaar. Vanuit financiën kijk je ook heel vaak naar valse stukken, wanneer is het gemaakt en wanneer is het gebruikt.
We maken er meer gebruik van. Bij zeden gaat erg veel over het internet heen, speelt zich digitaal af.
We zien veel telefoons die uitgelezen worden (ook laptops/iPads, etc). Team digi doet veiligstellen etc., maar het tactische deel doe je zelf.

Antwoorden door respondenten met veel ervaring met digitale sporen (N=8)

Daar werk ik bijna dagelijks mee. Ik doe alle tactische werkzaamheden. Ik bekijk veel uitgelezen telefoons. Veel tappen, verhoren. Open bronnenonderzoek.
Dagelijks ervaring met digitale sporen.
Dagelijkse kost voor mij als digitaal specialist. Ik heb geen ervaring in operationeel werk en een achtergrond als programmeur. Voor mij zijn dingen veel minder tijdrovend.
Digitaal zit in mijn bloed. Het eerste wat ik kreeg jaren geleden was een mooie Nokia telefoon. Ik wilde een smartphone. Dat mocht niet, want dat hoorde niet bij mijn functie. Ik vroeg: als ik twee zaken met internet zou oplossen, krijg ik dan een smartphone? Dat mocht. Het lukte. Analyse op internet gaf in twee dagen inzicht in twee zaken. Mijn chef draaide 180 graden om: nu moeten we alles met internet doen. Er zijn hoge verwachtingen. We moeten altijd de technische component erbij pakken.
Ik gebruik een iRN op de werkplek. Zeker bij evenementen kijken we wat er speelt. Ook wel bij specifieke zaken en dan komen ze bij mij om te zoeken. […] We gebruiken ook digitaal om mensen te bereiken en over zaken te informeren.
Ik gebruik het in mijn werk heel veel eigenlijk. Mijn crimeteam heeft geen kennis/kunde, dus dan vragen ze mij.
Ik werk er veel mee. Cybercrime is prioriteit nummer 1 bij het Openbaar Ministerie. Ik ben daarin opgeleid.
Vorig jaar 1300 PC's en 300 zaken onderzocht in Friesland. Er is meer ruimte voor digitaal. Je lost in snelle tijd meer zaken op.

Daarnaast waren antwoorden (deels) gericht op het gebruik van digitale sporen bij de politie in het algemeen. Ten derde kwam bij een deel van de respondenten de mogelijkheden, waarde en beperkingen van digitale sporen aan bod. Tot slot werd door sommige respondenten een vergelijking gemaakt tussen digitale en analoge sporen. Deze drie deelthema's komen achtereenvolgens in onderstaande drie tabellen aan bod.

Antwoorden over het gebruik van digitale sporen bij de politie (N=27)

Bij politie algemeen is er nog wel onbekendheid. Lastig om keuzes te maken, men weet niet wat te halen valt uit zo'n bron. Ook 'alles' doorzoeken is niet mogelijk. Digitale gegevens zijn niet altijd zwart/wit goed te duiden en dus vaak ondersteunend bewijs.
Binnen politie nog niet echt bekend waar je kansen liggen met betrekking tot digitale opsporing. Je loopt altijd achter de feiten aan.

Digitale component wordt steeds groter. We lopen achter de feiten aan. We kunnen wel bijscholen en bijscholen. We leiden wel mensen op, maar het wordt beperkt door mogelijkheden van Team Digitale Opsporing. Je mag niet zelf bij Team Digitale Opsporing telefoon uitlezen, daar moet iemand bij zijn. Wachttijden vallen nu wel mee. Dienst Regionale Recherche heeft eigen digitaal platform, waardoor je wel sneller wordt bediend. Als je dan telefoon hebt, dan gebruiken we UFED, daar moeten mensen dan weer handig in worden. Bij 18 GB aan data: wat zoek je dan en hoe zoek je dan. We zijn nu bezig om dat bij mensen tussen de oren te krijgen. Wat zijn de mogelijkheden en hoe verwoorden we dat dan in een pv. Er zijn verschillende zoekmogelijkheden. Cursus wordt straks gegeven door digitaal platform en Team Digitale Opsporing. Oudere garde vindt het altijd wat lastig.
Eerder nam je telefoon in beslag en leverde deze af. Nu bij de recherche ga je er zelf mee aan de slag.
Er is echt wel een drempel. Ik heb van collega's wel gehoord dat als aangifte wordt gedaan van de diefstal van een telefoon, dat de ene college haakjes ziet om uit te lopen en een ander denkt: dit is kansloos. Er is een groot gat. Er is winst te behalen om mensen bewust van te maken. Dat mensen weten: dit kan allemaal.
Er is een hele grote hang naar de traditionele kant. Ik ben eerder bang voor dat als we dat blijven doen, dat we dan weg geautomatiseerd worden. Alle gegevens worden ingevoerd en dan maakt een computer de analyse. Menselijk falen is vaak de reden, niet dat een computer een fout maakt. Strafrechtsketen kan gedigitaliseerd worden. Ik houd daar rekening mee. We moeten investeren, anders worden we weggevaagd. Er moet een beleidsstuk onder. Dat houdt ons tegen. Het beleid houdt ons tegen. Er zijn voldoende capabele mensen. Er zijn zelfs mensen die het wel aandurven. We moeten ze een digitale basis geven. Als je de basis kent, dan snap je vaak de rest ook. Moet politiebreed ook. Twintigers hebben dit vaak ook niet door.
Er is veel te halen, maar de kennis is beperkt. Vaak wordt iemand erbij gehaald die kennis heeft. Mensen willen geen fouten maken als ze het zelf doen.
Er is zoveel onwetendheid op de werkvloer. Ik heb andere inzichten. […] Ondanks dat ze mensen hebben die het zouden moeten weten, vragen ze me alsnog. Als er een bedreiging is online dan is het politiek gevoelig en moeten ze weten door wie berichten zijn geplaatst bijvoorbeeld.
Er zijn zaken die tussen het LMIO [Landelijk Meldpunt Internetoplichting], het cybercrimeteam én het crimeteam vallen. Dan is het wel oplichting, maar niet via Marktplaats, dus dan doet LMIO het niet. Als er communicatie is via Telegram, dan stopt LMIO. Volgens het cybercrimeteam is het in principe gewoon oplichting. Vervolgens zegt het crimeteam: dit zijn internationale bankrekeningnummers, wij weten het niet. Dus dan valt het tussen alle drie in.
Heel veel informatie uit te krijgen waar we nog niet veel kennis van hebben. Daar moet je de goede mensen en het goede materiaal voor hebben.
Ik heb iRN cursus gedaan. Dat duurde toen nog twee jaar voordat we zo'n computer kregen, dus toen wist ik niet meer hoe ik het geleerde moest toepassen. […] Heel jammer dat ik kennis kwijt ben. Ik weet niet meer precies hoe dat werkte. Vind ik jammer. Cursus was wel heel erg leuk. Ik had geen eigen Gmail of Facebook, na die cursus heb ik Facebook aangezet.
Ik vind dat een ieder een basiscursus moet volgen.
Ik vind dat het nog steeds een ondergeschoven kindje is en dat we er te weinig mee doen. Er zijn te weinig collega's die er iets vanafweten en er wordt te weinig aandacht aan gegeven. Het is naast forensisch-technisch en financieel de toekomst volgens mij.
Ik vind dat mensen er te weinig vanaf weten en dat het als een soort exotisch iets wordt beschouwd. Tegelijkertijd doen de mensen die er meer vanaf weten er nogal eens te 'spastisch' over.
In je eentje draai je van dit soort onderzoeken. Met zo'n twee of drie man gaat het sneller.
Je krijgt wel sneller ondersteuning heb ik gemerkt.
Lastig om de juiste mensen te pakken te krijgen. Er zijn ook weinig mensen die telefoons kunnen uitlezen. […] Met minimale capaciteit het maximale resultaat halen.
Mensen zoeken heel snel op hun computer naar de verdachte: "Ik kijk alleen maar even". Gewoon achter de werkplek doen ze vriendschapsverzoeken. Facebook maakt links tussen accounts; deze werkwijze is heel gevaarlijk. Op IP-adres kunnen er connecties worden gemaakt.
Per basisteam zouden we één iemand van het crimeteam moeten aanwijzen die zich mag verdiepen in digitale zaken. Ik krijg wel de ruimte daarvoor, maar wij zijn het enige team denk ik.
Tijd ontbreekt om er meer mee te doen.
Toegankelijkheid naar digitaal wordt steeds gemakkelijker. Collega's weten team digi steeds makkelijker te vinden. Timmeren goed aan de weg. Ze kunnen wel iets meer 'reclame' maken, over wat ze kunnen en doen.

Veel meer uit te halen dan we nu doen. Met name bij in beslag genomen gegevensdragers (mobiele telefoons). We zijn druk met tappen. Telefoons doen we als we tijd hebben. Hangt wel af van de afdeling waar je werkt. Bij de DRR is ook tijd en capaciteit een probleem maar wel meer doorlooptijd (en kan je dan prioriteren).
Vooral doen, op straat worden de kansen nog niet altijd gezien. Eerst digitaal bewust maken. Binnen alle lagen organisatie bekend maken met digitale sporen.
We doen er als politie soms niet altijd alles mee. Alles wat je in telefoon vindt kun je gebruiken in verhoor.
We lopen hopeloos achter.
We maken er te weinig gebruik van, van digitale sporen.
Wordt te weinig gebruikt, altijd omdat er te weinig kennis van is.

Antwoorden over de waarde, mogelijkheden en beperkingen van digitale sporen (N=24)

Beeldmateriaal kost veel tijd, en verschillende formats worden aangeleverd (extensies).
Chatcontact was laatst heel belangrijk in een zaak, live chatcontact. Dat was een heel belangrijke bron. Belangrijk bewijsstuk bij de zitting. Besef groeit dan van nut. Je wordt overstelpt met informatie. Vroeger had je met 100.000 kinderporno plaatjes al veel. Hoe ga je in hemelsnaam 12 TB classificeren en zoeken. Het wordt zo groot. Wat wil je en wat kun je nog. Daar is iemand een jaar mee bezig. Het is heel veel en moeilijk bij te houden. Wij hebben een informatiepoot die vergelijking kan maken, die links kan leggen, kan filteren, zodat we beter en sneller effectiever en efficiënter kunnen werken. Dat is landelijk nog niet zover. We willen het intern gaan organiseren, maar dat mag niet, omdat dat landelijk geregeld wordt qua zeden. Meldingen over diverse jaren landelijk koppelen. We willen nu landelijk actieve verdachten pakken, we komen er te laat achter dat iemand meerdere slachtoffers heeft gemaakt (in Summ-IT).
Digitale sporen kunnen snel weg zijn en gemanipuleerd worden. Moeilijk om grip op te krijgen. Moeilijk om analoog persoon aan digitale identiteit te koppelen.
Digitale sporen zijn soms heel waardevol. Het liegt niet. App-berichten, beelden. Je kunt heel veel halen. Justitie hecht er veel waarde aan. Ja, dat verwerk ik in mijn dossier en ik gebruik het voor mijn verhoren, daar kan ik verdachte mee confronteren.
Dit gaat in de toekomst natuurlijk veel vaker gebruikt worden.
Geweldig, de oplossing zit in digitale sporen in de toekomst.
Heeft veel bewijswaarde.
Het is tegenwoordig belangrijk, kan niet meer zonder.
Het maken van een script levert veel info op.
Het spoor is heel zwart-wit en duidelijk. De uitkomst is voor interpretatie vatbaar. Wie had de telefoon daadwerkelijk in handen? Het spoor zelf is zwart-wit.
Het stikt van de digitale sporen. Je kunt bellen voor MAC-adressen van de telefoons. Equens[41] kun je bellen voor wie op dat moment aan het pinnen was. Dienst Specialistische Recherche Toepassingen kun je bellen of er een satelliet is overgevlogen.[42]
Ik behandel rechtshulpverzoeken uit het buitenland. Vorderingen ontbreken vaak, op IP-adressen, etc. Dat is een gebrek voor een inhoudelijk verdachte verhoor. Door Open Source Intelligence opleiding heb ik geleerd dat er zoveel sporen te vinden zijn zonder dat je BOB-middelen hoeft in te zetten.
Ik heb nog geen positieve ervaring ermee dat het doorslaggevend is in een onderzoek.
Impact van het innemen van iemands telefoon is ingrijpende maatregel, dus zorgvuldig mee omgaan.
Je ontkomt er niet meer aan met de huidige technieken.

41 Equens is een Europese betalingsverwerker.

42 De Dienst Specialistische Recherche Toepassingen was een dienst van het voormalige Korps Landelijke Politiediensten (KLPD), en is in die vorm opgeheven per 1 januari 2013, bij de start van de Nationale Politie. (https://thesaurus.politieacademie.nl/Thesaurus/Term/4428, geraadpleegd 18 november 2019).

Je weet soms niet op welk moment je het wel/niet kunt gebruiken. Bij zeden ben je vaak te laat. Er gaat vaak tijd overheen en je start meestal met een getuige. Gegevens zijn dan soms al verloren gegaan.
Mensen zijn via internet veel makkelijker te vinden dan je zou denken. Familie is ook heel makkelijk te vinden. Is de familie gezellig uit eten geweest. Waar was dat. Traceren. Partner heeft vaak wel een Facebook account. Het kan heel snel gaan. Het kan LinkedIn zijn. Een telefoonnummer. Er is zo absurd veel dat je kunt vinden.
Met de telefoon heeft wel echt de toekomst, als je kijkt naar de jeugd is de telefoon hun leven.
Mijn ervaring is dat het heel veel oplevert, het gebruik van digitale sporen bedoel ik. Het levert ook heel veel input op voor verhoren. Digitaal levert heel veel op. Veel mensen maken gebruik van sociale media. Maar we moeten daar wel gebruik van maken.
Mooie resultaten mee gehaald in onderzoeken. In een zaak verklaarde verdachte dat hij zich op plaats X bevond, maar wij konden digitaal aantonen dat het plaats Y was. De rechter vond zijn verklaring vervolgens leugenachtig op dat punt. Positieve ervaring dus.
Over het algemeen is er heel veel uit te halen. Verschillende onderzoeken hebben tot relevante resultaten geleid met de inzet van digitale middelen, ook tot veroordelingen. Het zal steeds belangrijker worden.
Tactisch wordt meer digitaal.
Uit telefoons haalden we heel veel informatie, maar soms ook niks. Het heeft over het algemeen wel resultaten opgeleverd.
Vluchtig, er moet snel gehandeld worden.

Antwoorden over digitale sporen versus analoge sporen (N=7)

Analoog en digitaal gaan parallel.
Digitale sporen leveren in mijn ogen nu meer op dan klassieke opsporingsmethoden. Ik denk aan gegevens uit telefoons. Over de tap wordt sowieso weinig gezegd. Met de telefoon waant men zich nog veilig.
Het is lastiger. Je moet een vordering hebben, dingen regelen. Al het fysiek aanwezige kun je op papier zetten. Daar heb je geen officier van justitie voor nodig, gaat sneller.
Nog steeds worden er veel meer telefoons getapt dan internet tappen. Bij telefoons krijg je alleen gesprekken en sms'jes mee, niet Whatsapp. Je krijgt mee op welke site ze vaak kijken. Niet de inhoud daarvan. Alleen www.facebook.com. Je kunt wel verder kijken, maar er zijn maar weinig die dat kunnen bij de politie.
Normaal gesproken zouden we twee kanten bewandelen. Digitale wereld is tegenwoordig net zo belangrijk.
Op basis van telefoongegevens kun je al wel goed vaststellen hoe iemand beweegt. Uit telefoons haal je best veel informatie. Het is dus belangrijk om hier goed naar te kijken, vooral ook omdat de technische sporen, zoals DNA, er vaak niet zijn zodat je op andere wegen bent aangewezen, ook omdat er nogal eens geen getuigen zijn.
We zijn vaak in systemen moeilijk aan het zoeken, terwijl in open bronnen vaak heel makkelijk hetzelfde te vinden is. Het lijkt alsof we vroeger bijvoorbeeld overal zochten naar een telefoonnummer, behalve in het telefoonboek. Open bronnen vergeten we vaak voor dat soort gegevens.

Bijlage 9. Gegeven antwoorden in de herhaalvragenlijst op de stellingen over knelpunten

De knelpunten die bij de beantwoording van deelvraag 1 naar voren kwamen (zie hoofdstuk 4) zijn in de vragenlijst, enkele weken na het casusonderzoek, voorgelegd aan de respondenten. In onderstaande tabel zijn alle antwoorden weergegeven (N=54, in procenten).

	Helemaal mee oneens	Enigszins mee oneens	Niet mee oneens, niet mee eens	Enigszins mee eens	Helemaal mee eens
Ik weet hoe ik met digitale sporen moet werken	1,9	16,7	13,0	46,3	22,2
Ik ben onbekend met de mogelijkheden die digitale sporen bieden	27,8	27,8	9,3	29,6	5,6
Ik zie de potentie van digitale sporen	0	1,9	0	25,9	72,2
Er zijn voldoende faciliteiten om met digitale sporen te werken	14,8	18,5	25,9	22,2	18,5
Ik ben bang om fouten te maken met digitale sporen	16,7	27,8	24,1	24,1	7,4
Werken met digitale sporen is gebruiksvriendelijk	9,3	33,3	40,7	13,0	3,7
Digitale experts zijn te druk om mij te helpen met het werken met digitale sporen	25,9	27,8	37,0	5,6	3,7
Ik ben onbekend met de bevoegdheden die ik nodig hem om met digitale sporen te werken	16,7	29,6	22,2	25,9	5,6
Er is voldoende jurisprudentie om met digitale sporen te werken	0	22,2	53,7	20,4	3,7
Data uit digitale gegevensdragers zijn omvangrijk om mee te werken	1,9	9,3	14,8	48,1	25,9
Er is onvoldoende capaciteit om met digitale sporen te werken	1,9	22,2	22,2	33,3	20,4
Digitale sporen zijn betrouwbaar	0	9,3	25,9	48,1	16,7
Ik heb interesse in het gebruik van digitale sporen	0	0	9,3	50,0	40,7

Ik ben onzeker over mijn kennis over digitale sporen	18,5	25,9	22,2	27,8	5,6
Werken met digitale sporen brengt ongewenste veranderingen in politiewerk met zich mee	44,4	31,5	13,0	3,7	7,4

Bijlage 10. **Antwoorden op kennisvragen**

In onderstaande tabellen staan de antwoorden van alle respondenten op twee vragenblokken: een vragenblok over digitale sporen en een vragenblok over het benutten van sporen uit gegevensdragers.

N=76, in procenten. De modus is groen gemarkeerd.	**Helemaal mee oneens**	**Enigszins mee oneens**	**Niet mee oneens, niet mee eens**	**Enigszins mee eens**	**Helemaal mee eens**
Ik weet welke digitale sporen van belang zijn voor opsporingsonderzoek	0	14,5	9,2	43,4	32,9
Ik weet hoe de 7 W's (wie, wat, waar, waarmee, welke wijze, wanneer, waarom) kunnen worden toegepast om de relevantie van digitale sporen te bepalen	1,3	13,2	19,7	39,5	26,3
Ik ken mijn eigen beperking(en) bij het verrichten van een opsporingsonderzoek naar digitale criminaliteit	0	2,6	3,9	43,4	50,0
Ik weet hoe ik moet handelen wanneer ik bij het verrichten van opsporingsonderzoek naar digitale criminaliteit onvoldoende kennis heb	0	6,6	9,2	40,8	43,4
Ik weet wat 'vluchtige gegevens' zijn	6,6	6,6	9,2	39,5	38,2
Ik ken de bevoegdheden tot inbeslagname van gegevensdragers	2,6	7,9	10,5	52,6	26,3
Ik weet welke gegevensdragers op een PD relevant zijn voor inbeslagname	1,3	5,3	5,3	57,9	30,3
Ik weet welke gegevensdragers kunnen worden uitgelezen	2,6	3,9	10,5	47,4	35,5
Ik weet tijdens een onderzoek wanneer het nuttig/noodzakelijk is om gegevensdragers uit te lezen	1,3	7,9	11,8	52,6	26,3
Ik weet hoe ik softwarepakketten moet gebruiken om digitale sporen te analyseren	30,3	31,6	11,8	14,5	11,8
Ik weet hoe ik de bevindingen van digitaal sporenonderzoek moet vastleggen (dossiervorming)	14,5	26,3	17,1	18,4	23,7
Ik weet welk type informatie je kunt vinden op welk type internet bron	6,6	17,1	31,6	30,3	14,5
Ik weet waar ik op internet moet zoeken om persoonsgegevens te achterhalen	3,9	17,1	19,7	42,1	17,1

N=76, in procenten. De modus is groen gemarkeerd.	**Helemaal mee oneens**	**Enigszins mee oneens**	**Niet mee oneens, niet mee eens**	**Enigszins mee eens**	**Helemaal mee eens**
Ik weet waar ik op internet moet zoeken om bedrijfsgegevens te achterhalen	5,3	17,1	15,8	42,1	19,7
Ik weet hoe ik als politiemedewerker zo weinig mogelijk sporen kan achterlaten bij het zoeken op internet	11,8	14,5	14,5	35,5	23,7

Bijlage 11. **Correlaties**

Tabel 1: Positief geformuleerde knelpunten (N=31)

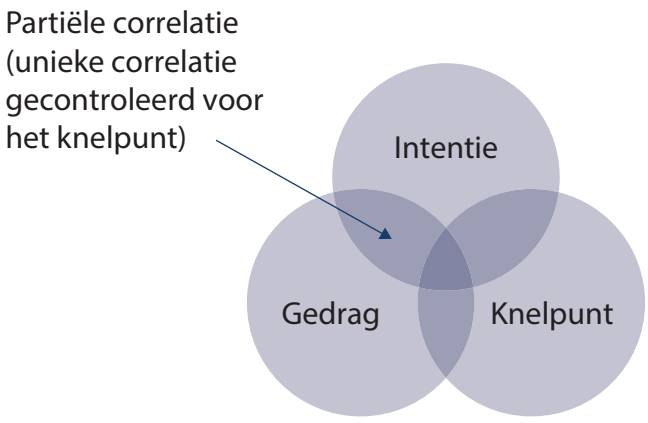
	Intentie	**Gedrag**
Ik zie de potentie van digitale sporen	.142	-.126
Ik heb interesse in het gebruik van digitale sporen	-.141	-.064
Ik weet hoe ik met digitale sporen moet werken	.526**	.468**
Digitale sporen zijn betrouwbaar	-.017	.056
Er zijn voldoende faciliteiten om met digitale sporen te werken	.140	.157
Er is voldoende jurisprudentie om met digitale sporen te werken	.127	.086
Werken met digitale sporen is gebruiksvriendelijk	.194	.369*

Tabel 2: Negatief geformuleerde knelpunten (N=31)

	Intentie	**Gedrag**
Data uit digitale gegevensdragers zijn omvangrijk om mee te werken	.301	-.134
Er is onvoldoende capaciteit om met digitale sporen te werken	.028	-.032
Ik ben onbekend met de mogelijkheden die digitale sporen bieden	-.445*	-.168
Ik ben onzeker over mijn kennis over digitale sporen	-.188	-.011
Ik ben onbekend met de bevoegdheden die ik nodig heb om met digitale sporen te werken	-.322	-.088
Ik ben bang om fouten te maken met digitale sporen	-.480**	-.335
Werken met digitale sporen brengt ongewenste veranderingen in politiewerk met zich mee	.092	.238
Digitale experts zijn te druk om mij te helpen met het werken met digitale sporen	-.088	-.059

**Significant met een p-waarde <.01

*Significant met een p-waarde <.05



Tabel 3: Partiële correlatie tussen intentie en gedrag (N=31)

	Intentie	**Gecontroleerd voor**
Gedrag	.359	-
	.376	Ik zie de potentie van digitale sporen
	.358	Ik heb interesse in het gebruik van digitale sporen
	.170	Ik weet hoe ik met digitale sporen moet werken
	.358	Digitale sporen zijn betrouwbaar
	.355	Er zijn voldoende faciliteiten om met digitale sporen te werken
	.357	Er is voldoende jurisprudentie om met digitale sporen te werken
	.329	Werken met digitale sporen is gebruiksvriendelijk
	.417	Data uit digitale gegevensdragers zijn omvangrijk om mee te werken
	.356	Er is onvoldoende capaciteit om met digitale sporen te werken
	.339	Ik ben onbekend met de mogelijkheden die digitale sporen bieden
	.370	Ik ben onzeker over mijn kennis over digitale sporen
	.339	Ik ben onbekend met de bevoegdheden die ik nodig heb om met digitale sporen te werken
	.251	Ik ben bang om fouten te maken met digitale sporen
	.365	Werken met digitale sporen brengt ongewenste veranderingen in politiewerk met zich mee
	.356	Digitale experts zijn te druk om mij te helpen met het werken met digitale sporen

Bijlage 12. Het verhogen van digitale kennis en de invloed van opleidingen

Auteur: Jan Aink

1. Inleiding

Digitale sporen zijn overal. In toenemende mate laten wij digitale sporen achter. De verwachting is dat dit steeds zal toenemen, waarbij verwezen wordt naar de opkomst van het Internet of Things en kunstmatige intelligentie (Henseler, 2017). De ontwikkelingen in onze steeds veranderende maatschappij stellen hoge eisen aan de rechtstaat. Het toekomstbestendig opleiden van opsporingsambtenaren heeft daarbij volgens een brief van de Minister van Justitie en Veiligheid van 15 juni 2018 de volle aandacht. In de moderne politieorganisatie zijn vaardigheden vereist om, onder meer, cybercrime slagvaardig tegen te kunnen gaan (Kamerstukken 29628, nr. 784). In de strategische onderzoeksagenda van de politie over de jaren 2019 tot 2022 worden als grote uitdagingen genoemd hoe digitale vaardigheden voor opsporingsambtenaren het beste kunnen worden onderwezen, op peil kunnen worden gebracht en kunnen worden onderhouden (Nationale Politie, 2019).

Het doel van dit deelonderzoek is om inzicht te krijgen in hoeverre effecten waargenomen kunnen worden tussen het gevolgd hebben van een of meerdere cursusdagen op het vlak van digitaal politiewerk en de intentie tot en het gebruik van digitale sporen. De centrale vraag luidt daarbij als volgt: 'In hoeverre zijn er verschillen met betrekking tot de intentie tot en het gebruik van digitale sporen in opsporingsonderzoeken tussen opsporingsambtenaren die een cursus met betrekking tot digitale criminaliteit hebben gevolgd en opsporingsambtenaren die geen cursussen hebben gevolgd?'

Om de hoofdvraag te beantwoorden zijn zeven hypothesen opgesteld en een aanvullende deelvraag. Om de onderlinge samenhang en verklaarde variantie van het conceptueel model te meten is de volgende deelvraag opgesteld: 'Wat is de voorspellende waarde van de concepten attitude, subjectieve norm, gepercipieerde gedragscontrole, gepercipieerd nut en gepercipieerd gebruiksgemak op de sterkte van de gedragsintentie en het daadwerkelijk gebruik van digitale sporen?' Deze concepten komen uitgebreid aan bod in de volgende paragraaf. Om de hypothesen te toetsen en de deelvraag te

beantwoorden is een secundaire data-analyse uitgevoerd op de in het methodenhoofdstuk besproken dataset. Deze dataset (N=76) bestaat uit een groep die wel een cursus heeft gevolgd op het digitale vlak (N=46) en een groep die geen een cursus heeft gevolgd (N=30).

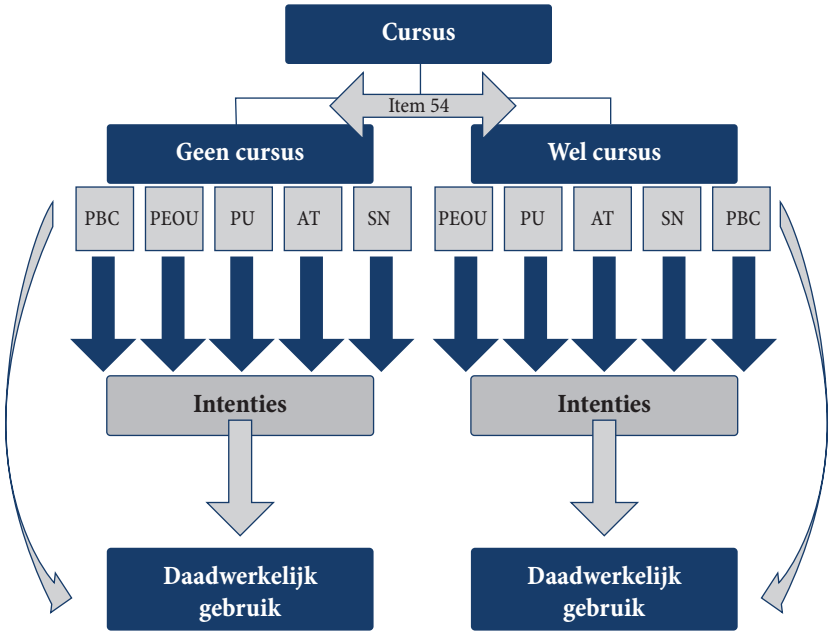
2. Theoretisch kader

Het bestendig aanleren en vervolgens toepassen van (digitale) vaardigheden die nodig zijn in de moderne politieorganisatie gaat in wezen om het bewerkstelligen van gedragsverandering. De theorievorming op het gebied van gedragsverandering kan worden ingedeeld bij het domein van de psychologie als zijnde de wetenschap die zich bezig houdt met het bestuderen van menselijk gedrag.

Er is voor wat betreft de theoretische onderbouwing aansluiting gezocht bij twee sociaalpsychologische intentiemodellen. Het gaat hierbij om de Theory of Planned Behavior (TPB) en het Technology Acceptance Model (TAM). Wat beide modellen verenigt, is dat beide uitgaan van de veronderstelling dat een hoge mate van gedragsintentie om het beoogde gedrag uit te voeren een goede voorspeller is dat dit ook daadwerkelijk gebeurd.

Vertaalt binnen de context van dit onderzoek veronderstellen we op basis van de TPB (Ajzen, 1985) dat (a) een positieve attitude (houding) ten opzichte van het gebruik van digitale sporen, (b) een hoge ervaren subjectieve norm (wat anderen – die belangrijk zijn voor een persoon – denken over het uit te voeren gedrag) met betrekking tot het gebruik hiervan, en (c) gepercipieerde gedragscontrole (de perceptie die men heeft over de eigen vaardigheden om het beoogde gedrag uit te voeren) goede voorspellers te zijn voor gedragsintentie. Een sterke gedragsintentie is op zijn beurt weer een goede voorspeller voor het daadwerkelijk gebruik. In het TAM worden, naast attitude, het gepercipieerde nut en het gepercipieerde gebruiksgemak aangemerkt als belangrijke voorspellers voor gedragsintentie (Davis, 1989).
De hiervoor genoemde voorspellers, de gedragsintentie en het daadwerkelijk gebruik zijn in een conceptueel model gegoten, zie .
De bijbehorende hypothesen zijn daaronder vermeld. Voor aanvullende informatie over de besproken theorieën en de relatie tussen deze theorieën en de onderzoekscontext verwijzen wij naar het – aan het hoofdonderzoek verwante – afstudeeronderzoek van Aink (2019).

Figuur 1: Conceptueel model deelonderzoek



Notitie. PBC (perceived behavioural control; gepercipieerde gedragscontrole), PEOU (perceived ease of use; gepercipieerd gebruiksgemak), PU (perceived usefulness; gepercipieerd nut), AT (attitude), SN (subjectieve norm).

In dit deelonderzoek worden de vijf voorspellers van de gedragsintentie, de gedragsintentie zelf en het daadwerkelijk gebruik van digitale sporen gemeten en vergeleken tussen beide groepen. Ter beantwoording van de hoofdvraag is een zevental hypothesen opgesteld. Door middel van de hypothesen wordt getoetst of de voorspellers van gedragsintentie, die zijn ontleend aan de TPB en het TAM, verschillen tussen politiemensen die wel of geen cursus hebben gevolgd op het digitale vlak. De hypothesen zijn hieronder weergegeven.

H1. Opsporingsambtenaren die een of meer cursusdagen op het digitale vlak hebben gevolgd rapporteren een hogere positieve attitude om digitale sporen te gebruiken dan opsporingsambtenaren die geen cursussen hebben gevolgd op het digitale vlak.

H2. Opsporingsambtenaren die een of meer cursusdagen op het digitale vlak hebben gevolgd rapporteren een hogere subjectieve norm met betrekking tot het gebruik van

digitale sporen in opsporingsonderzoeken dan opsporingsambtenaren die geen cursussen hebben gevolgd op het digitale vlak.

H3. Opsporingsambtenaren die een of meer cursusdagen op het digitale vlak hebben gevolgd rapporteren een hogere gepercipieerde gedragscontrole met betrekking tot het gebruik van digitale sporen in opsporingsonderzoeken dan opsporingsambtenaren die geen cursussen hebben gevolgd op het digitale vlak.

H4. Opsporingsambtenaren die een of meer cursusdagen op het digitale vlak hebben gevolgd rapporteren een hoger gepercipieerd gebruiksgemak met betrekking tot het gebruik van digitale sporen in opsporingsonderzoeken dan opsporingsambtenaren die geen cursussen hebben gevolgd op het digitale vlak.

H5. Opsporingsambtenaren die een of meer cursusdagen op het digitale vlak hebben gevolgd rapporteren een hoger gepercipieerd nut met betrekking tot het gebruik van digitale sporen in opsporingsonderzoeken dan opsporingsambtenaren die geen cursussen hebben gevolgd op het digitale vlak.

H6. Opsporingsambtenaren die een of meer cursusdagen op het digitale vlak hebben gevolgd rapporteren een hogere intentie met betrekking tot het gebruik van digitale sporen in opsporingsonderzoeken dan opsporingsambtenaren die geen cursussen hebben gevolgd op het digitale vlak.

H7. Opsporingsambtenaren die een of meer cursusdagen op het digitale vlak hebben gevolgd maken meer gebruik van digitale sporen dan opsporingsmedewerkers die geen cursussen op het digitale vlak hebben gevolgd.

3. Methoden

Voor een uitvoerige beschrijving van de (data-analyse en) methoden wordt verwezen naar hoofdstuk 3 van dit rapport en naar het afstudeerrapport van Aink (2019).

In de dataset zijn de tien keuzemomenten als afzonderlijke variabelen weergegeven. De scores zijn gecodeerd als '0' zijnde de keuze voor een analoog spoor en als '1' zijnde de keuze voor een digitaal spoor. Op basis van deze tien variabelen is een nieuwe somvariabele samengesteld waarin het totaal van de keuze voor een digitaal spoor is opgeteld. Nu deze nieuwe gesommeerde variabele op intervalniveau is weergegeven en de verdeling normaal is gebleken, zijn de gemiddelden tussen beide groepen door middel van de independent samples *t*-test geanalyseerd op significantie. Het significantieniveau is vastgesteld op ,05. Uit een analyse van de ruwe data bleek met betrekking tot het experiment dat nagenoeg alle (N=74, 97,4%) proefpersonen ervoor kozen om onderzoek te doen naar een telefoon met 18 GB aan data in tegenstelling tot het onderzoeken van dertig verhuisdozen met administratie. Gesteld kan worden dat dit keuzemoment een

zeer laag discriminerend vermogen bezit. Daarom is ervoor gekozen om keuzemoment acht eruit te filteren en uit te gaan van de negen resterende valide keuzemomenten.

De voorspellers van gedragsintentie zijn gemeten aan de hand van de vragenlijst. In de analyses zijn de scores op de (al dan niet samengestelde) items geanalyseerd door gemiddelden te berekenen en vervolgens deze scores tussen de twee te onderscheiden groepen te vergelijken. Om te toetsen of de aangetroffen verschillen significant zijn, zijn de scores geanalyseerd met behulp van de independent samples *t*-test bij een normale verdeling en de Mann Whitney U-test bij een scheve verdeling, waarbij de testvariabele bestond uit de (gesommeerde en samengestelde) items en de splitsingsvariabele bestond uit de gerapporteerde cursusdagen. Een gemeten verschil tussen gemiddelden is significant vanaf $p<,05$. Om de onderlinge samenhang en verklaarde variantie van het conceptueel model te analyseren is gebruikgemaakt van een enter-regressieanalyse. Alle analyses zijn uitgevoerd met het statistische softwarepakket SPSS.

4. Resultaten

In deze paragraaf zijn de resultaten van het deelonderzoek beschreven. Ten eerste kijken we naar de verschillen tussen doelgroepen wat betreft (a) voorspellers, (b) intentie en (c) gedrag (par. 4.1). Daarbij wordt eveneens gekeken naar in hoeverre de gestelde hypothesen aangenomen kunnen worden. Ten tweede beschouwen we de gemeten variabelen in hun geheel door middel van het presenteren van de uitkomsten uit de regressieanalyses (par. 4.2).

4.1 Verschillen tussen doelgroepen

In tabel 1 zijn de cijfermatige resultaten weergegeven met betrekking tot de uitgevoerde independent samples *t*-toetsen en de Mann Whitney U betreffende de hypothesen 1 tot en met 7.

Tabel 1: Resultaten t-toetsen en Mann Whitney U-toetsen.

	Cursus	N	M/Mdn	M (verschil)	Verdeling	*t*-toets	Mann Whitney
PBC	Niet	30	24,10		Normaal	n.v.t.	,000*
	Wel	46	46,64		Scheef		
AT	Niet	30	26,23		Scheef	n.v.t.	,000*
	Wel	46	46,50		Scheef		
SN	Niet	30	13,967	2,300	Normaal	,006	n.v.t.
	Wel	46	16,267		Normaal		
PEOU	Niet	30	30,70		Normaal		,021*
	Wel	46	42,14		Scheef		

PU	Niet	30	31,23		Scheef	n.v.t.	,010*
	Wel	46	43,24		Scheef		
INT	Niet	30	27,02		Scheef	n.v.t.	,000*
	Wel	46	45,32		Scheef		
GEB	Niet	30	6,3103	-,0277	Normaal	,896	n.v.t.
	Wel	46	6,2826		Normaal		
GEB mi-nus8	Niet	30	5,3261	-,0072	Normaal	,370	n.v.t
	Wel	46	5,3333		Normaal		

Notitie. PBC (perceived behavioural control; gepercipieerde gedragscontrole), AT (attitude), SN (subjectieve norm), PEOU (perceived ease of use; gepercipieerd gebruiksgemak), PU (perceived usefulness; gepercipieerd nut), INT (gedragsintentie), GEB (gebruik).
*p < ,05.

Eerst bespreken we de voorspellers die zijn ontleend aan de TPB. Op basis van de *t*-toets en de Mann Whitney U werden de grootste effecten gevonden op attitude en gepercipieerde gedragscontrole, terwijl de grootte van het effect op de subjectieve norm, hoewel significant, beperkt is gebleven.[43] Aan de hand van de Mann Whitney U-toets op attitude kwam naar voren dat de groep die wel een cursus had gevolgd (Mdn=46,50) hoger scoorde dan de groep die geen cursus (*Mdn*=26,23) had gevolgd (*U*=322, *Z*=-4,020, *p*<,001). De groep die wél een cursus had gevolgd rapporteerde daarnaast een significant hogere score (*Mdn*=46,64) op de gepercipieerde gedragscontrole ten opzichte van de groep die geen cursus (*Mdn*=24,10) had gevolgd (*U*=258, *Z*=-4,461, *p*<,001). In verband met een normale verdeling van de scores op de subjectieve norm is de independent-samples *t*-toets uitgevoerd. De gemiddelde score op dit concept van de groep die één of meer cursusdagen heeft gevolgd (M=16,2667) is significant hoger (*p*=,006) dan de groep die geen cursusdagen heeft gevolgd (M=13,9667). Daarmee worden de eerste drie hypothesen bevestigd.

Nu volgen de voorspellers van het TAM. Op de concepten gepercipieerd gebruiksgemak en gepercipieerd nut zijn tussen de twee groepen significante verschillen waargenomen. De groep die een cursus volgde had een sterk hogere score op de belangrijkste voorspellers van de gedragsintentie. Voor het gepercipieerde gebruiksgemak werd op een Likertschaal van zeven punten gevraagd in hoeverre het moeilijk of makkelijk is om de komende maand digitale sporen te gebruiken om aan een zaak te werken (item 72). Uit de Mann Whitney-toets bleek dat de groep respondenten die een cursus had gevolgd (*Mdn*=42,14) het werken met digitale sporen als eenvoudiger rapporteerde

43 Dat voor subjectieve norm een beperkter effect is gemeten lag in de lijn der verwachting. Het is immers niet te verwachten dat het volgen van een cursus een sterk effect zal sorteren op de perceptie die de individuele cursusdeelnemer heeft van de heersende norm die geldt binnen de rest van de werkvloer.

dan de (*U*=456, *Z*=-2,30, *p*=,021) groep die geen cursus had gevolgd (*Mdn*=30,70). Voor het concept gepercipieerd nut werd op een Likertschaal van zeven punten aan de respondenten gevraagd in hoeverre zij het nutteloos of nuttig vinden om de komende maand digitale sporen te gebruiken om aan een zaak te werken (item 60). Uit de Mann Whitney-toets bleek dat de groep die wel een cursus had gevolgd (*Mdn*=43,24) het werken met digitale sporen als nuttiger inschaalden dan de (*U*=937, *Z*=-2,573, *p*=,01) groep die geen cursus had gevolgd (*Mdn*=31,23). Hypothesen 4 en 5 kunnen daarmee worden bevestigd.

Daarnaast hangt het volgen van een cursus, in lijn met de verwachting, samen met intentie tot gebruik van digitale sporen. Het betrof een groot en significant effect. Uit de Mann Whitney-toets kwam naar voren dat de groep die wel een cursus had gevolgd (*Mdn*=45,32) significant hoger scoorde op intentie (*U*=345,5, *Z*=-3,616, $p < ,001$) dan de groep die geen cursus had gevolgd (*Mdn*=27,02). Hypothese 6 wordt daarmee bevestigd.

Het daadwerkelijk gebruik van digitale sporen, zoals dit is gemeten door het experiment, hangt tegen de verwachting in niet samen het volgen van een cursus. Hypothese 7 kan daarom niet worden aangenomen. De gemiddelde score voor het aantal ingezette digitale keuzemomenten voor de groep die wel een cursus had gevolgd (M=6,2558) was lager dan de groep die geen cursus had gevolgd (M=6,3101). Het gevonden verschil was klein en niet significant. Na de toegepaste correctie met betrekking tot keuzemoment acht was de gemiddelde score van de groep die wel een cursus had gevolgd lager (M=5,3261) dan die van de groep die geen cursus had gevolgd (M=5,3333), maar niet significant.

4.2 Resultaten regressieanalyses

In de vorige paragraaf zijn aan de hand van de opgestelde hypothesen de 'losse' concepten getoetst van de TPB en het TAM. In deze paragraaf worden de onderlinge samenhang en verklaarde variantie van het conceptueel model bezien, alsook die van de twee theorieën afzonderlijk. Hiermee wordt getracht de geformuleerde deelvraag te beantwoorden.

Door middel van een enter-regressieanalyse is gemeten welk van de concepten binnen de populatie van opsporingsambtenaren, zoals deze zijn opgesomd in het conceptueel model, de grootste voorspellende waarde hebben met betrekking tot (de sterkte van) de gedragsintentie. De attitude, subjectieve norm, gepercipieerde gedragscontrole, gepercipieerd gebruiksgemak en gepercipieerd nut werden als onafhankelijke variabelen ingevoerd, waarbij eerst de sterkte van de gedragsintentie en daarna het (gecorrigeerde) gebruik als afhankelijke variabele werd ingevoerd in de enter-regressieanalyse. In tabel 2 zijn de resultaten weergegeven.

Tabel 2 Uitkomsten regressieanalyse conceptueel model

Model	B	Std. Error	Beta	T	Sig.
(Constant)	-4,523	1,759		-2,571	,012
Attitude	-,163	,179	-,110	-,910	,366
Subjectieve norm	,423	,091	,444	4,644	,000
Gepercipieerde gedragscontrole	,538	,109	,465	4,931	,000
Gepercipieerd nut	,721	,387	,190	1,863	,067
Gepercipieerd gebruiksgemak	,043	,227	,019	,189	,851

Uit de enter-regressieanalyse blijkt dat 65% (adjusted R^2=,650) van de variantie op de sterkte van de gedragsintentie kon worden verklaard door de bovengenoemde voorspellers. De verklaarde variantie van het model voor de sterkte van de gedragsintentie, zoals weergegeven in het conceptueel model, is significant, F(5, 67)=27,69, p<,001, R^2=,674. Het conceptueel model heeft dus een sterk voorspellende waarde. De concepten gepercipieerde gedragscontrole en subjectieve norm dragen echter als enige significante voorspellers bij aan de voorspelling van de sterkte van de gedragsintentie, p<,001.

De overige concepten attitude, gepercipieerd gebruiksgemak en gepercipieerd nut dragen in dit regressiemodel niet significant bij aan de voorspellende waarde van de gedragsintentie. De theorie die binnen de context van dit onderzoek de sterkst voorspellende waarde lijkt te hebben is de TPB. Om deze reden is ervoor gekozen om de theorieën ook afzonderlijk te analyseren.

Als in navolging van de TPB attitude, subjectieve norm en gepercipieerde gedragscontrole als voorspellers worden ingevoerd dan blijkt dat deze theorie 64% (adjusted R^2=,644) van de variantie op de sterkte van de gedragsintentie verklaart. De verklaarde variantie van het model voor de sterkte van de gedragsintentie, volgens de TPB, is significant, F(3, 70)=45,09, p<,001, R^2=,659. De voorspellers van het TAM (attitude, gepercipieerd gebruiksgemak en gepercipieerd nut) verklaren 41% van de variantie op de sterkte van de gedragsintentie. De bovenvermelde berekeningen zijn ook op dezelfde wijze per theorie uitgevoerd, waarbij de afhankelijke variabele 'intentie' is veranderd in 'gebruik gecorrigeerd'. Uit deze resultaten blijkt geen van de theoretische modellen een significante proportie van de variantie van het gebruik van digitale sporen te verklaren.

De slotsom luidt dat het regressiemodel dat is opgesteld aan de hand van TPB 64% van de variantie op de sterkte van de gedragsintentie verklaard ten opzichte van de 65% verklaarde variantie door de voorspellers uit het (geïntegreerde) conceptueel model. Beide modellen hebben een sterke voorspellende waarde en verschillen nauwelijks.

5. Conclusie, discussie en aanbevelingen

In deze paragraaf staan de conclusie, discussie en aanbevelingen centraal. Voordat we daarop ingaan moet worden vastgesteld dat het deelonderzoek, net als het hoofdonderzoek, een aantal beperkingen kende. Ten eerste zijn er relatief weinig respondenten die hebben meegewerkt aan het onderzoek. Ten tweede zijn de voorspellers van de TPB en het TAM soms gemeten aan de hand van een enkel item. Dit heeft mogelijk zijn weerslag op de validiteit en betrouwbaarheid van de resultaten. Het is dan ook aan te bevelen om in vervolgonderzoek gebruik te maken van vragenlijsten die de items uit beide theorieën expliciet meten. Ten derde ligt er een beperking in de wijze waarop gedrag is geoperationaliseerd. Het is bovendien de vraag of de groep proefpersonen die aan het experiment en de vragenlijst hebben deelgenomen als een representatieve groep kan worden beschouwd. Tot slot is de vragenlijst afgenomen na afloop van het experiment. Deelname aan het experiment kan proefpersonen in een 'digitale' mindset hebben gebracht, waardoor de vragenlijst mogelijk anders zou zijn ingevuld als deze los van, of voorafgaand aan, het experiment was verspreid. Het is belangrijk om met dergelijke beperkingen rekening te houden bij het interpreteren van navolgende.

Hoewel de groep die een cursus had gevolgd een significant hogere score rapporteerde op de gedragsintentie, liet deze groep geen hogere score zien bij het daadwerkelijk benutten van digitale sporen. Dat is opvallend en tegen de verwachting. Dit geldt temeer nu voor de groep die een cursus had gevolgd ook een sterk verhoogde score is gemeten op de gepercipieerde gedragscontrole. Een hogere gerapporteerde gedragscontrole heeft blijkens de TPB immers (naast intentie) een rechtstreeks effect op het daadwerkelijk overgaan tot het beoogde gedrag (Ajzen, 1985). Deze voorspeller heeft kennelijk in dit onderzoek ook geen effect op het daadwerkelijk gebruik van digitale sporen. De verwachte samenhang met de verhoging van het beoogde gedrag is dus in dit onderzoek uitgebleven.

Ter verklaring hiervoor is dieper in de literatuur gezocht en daarbij zijn kritiekpunten op de sociaalpsychologische intentiemodellen gevonden. Zo is er in de literatuur op gewezen dat de sterke correlatie tussen intentie en gedragsverandering met name ziet op bewust geïnitieerd gedrag. Daarbij wordt in mindere mate rekening gehouden met gewoontegedrag en geautomatiseerde processen. Zo blijkt uit onderzoek dat gedragsintenties uiteindelijk slechts 20 tot 30% voorspellen van de beoogde gedragsverandering (Armitage & Conner, 2001). De kracht van nieuwgevormde intenties blijkt vaak niet sterk genoeg om het automatisme van de gewoonte te kunnen onderdrukken (Webb & Sheeran, 2006).

Het is mogelijk dat bij het werken aan opsporingsonderzoeken geautomatiseerde processen en/of gewoontegedrag bovengemiddeld aanwezig zijn. Dit kan ertoe leiden dat de sterk verhoogde gedragsintenties zich uiteindelijk (toch) niet uitbetalen in de beoogde gedragsverandering. Het is dus maar zeer de vraag of een breed in de organisatie

uitgerolde (basis)cursus en/of opleiding ook daadwerkelijk de beoogde gedragsverandering oplevert. Er kan daarmee echter niet gezegd worden dat het volgen van een cursus geen enkel positief effect heeft. Intenties kunnen namelijk volgens de literatuur als een noodzakelijke (maar geen voldoende) voorwaarde voor de beoogde gedragsverandering worden beschouwd (Armitage & Conner, 2001). Met andere woorden: als de gedragsintentie ontbreekt, zal het beoogde gedrag in ieder geval niet optreden. De uitdaging is erin gelegen om het gat tussen de gedragsintentie en het beoogde gedrag zoveel mogelijk te dichten. Volgens de literatuur kunnen implementatie-intenties daar helpend in zijn (Gollwitzer, 1999). Hierna wordt dieper op deze theorie ingegaan en zal middels aanbevelingen worden getracht handen en voeten te geven aan het dichten van de kloof.

Op basis van de implementatie-intentietheorie worden gedragsintenties eerder en beter omgezet in gedrag als er vooraf wordt ingegaan op de specifieke situatie waarin het beoogde gedrag het beste kan worden uitgevoerd. Deze specifieke situaties bevinden zich in de scope van dit onderzoek uiteraard binnen de context van de opsporingsonderzoeken. Er zal bijvoorbeeld in een trainings-/opleidingssetting met een digitale context kunnen worden getraind in het bepalen van oplossingsrichtingen/-strategie en het benutten van mogelijkheden en kansen. Volgens de theorie van de implementatie-intentie zal dan in een toekomstige (soortgelijke) casus het schema van het werken met digitale sporen – en de daarbij behorende oplossingsrichting – automatisch kunnen worden geactiveerd. In dat geval is er voor de opsporingsambtenaar geen bewuste aandacht meer nodig om een digitale oplossingsvariant als gedragsrepertoire op te roepen (Gollwitzer, 1999; Webb & Sheeran, 2008).

Uit onderzoek blijkt verder dat implementatie-intenties niet alleen helpend zijn om gewoontegedrag te doorbreken, maar ook om nieuwe gewoontes aan te leren (Holland, Aarts & Langendam, 2006). Daarnaast is volgens de ontwikkelingspsychologische literatuur 'active learning' een effectieve strategie voor het aanleren van nieuwe kennis en/of vaardigheden. De cursist heeft hierbij een actieve rol in het leerproces. Hierbij wordt uitgegaan hoe actiever een cursist bezig is met de aan te leren stof, hoe beter deze informatie wordt. Een cursist is door toepassing van de principes van 'active learning' bovendien in staat om de aangeleerde kennis en/of vaardigheden in verschillende contexten toe te passen. Bovendien kan door meer te 'doen' het handelen in het brein ook worden neergelegd als een geautomatiseerd proces, waardoor het beoogde gedrag zonder (al te veel) bewuste aandacht worden uitgevoerd. Ook (en misschien wel vooral) bij het aanleren van digitale vaardigheden geldt dus het adagium: Learning by doing! (Van Diepen, Stefanova & Miranowicz, 2009).

Opsporingsambtenaren door hele politieorganisatie heen, dus in de volle breedte, mee laten draaien in opsporingsonderzoeken met een digitale component en – indien er wordt getraind – uit te gaan van een concrete (cyber)opsporingscasus, zal volgens de theorie maken dat het werken met digitale sporen (al dan niet met tussenkomst van

TDO) steeds meer kan verworden tot een geautomatiseerd proces. Er wordt daarom aanbevolen om te trainen met in de praktijk (veelvoorkomende) casuïstiek op het gebied van digitale criminaliteit. Een praktisch voorbeeld is om tijdens de Integrale Beroepsvaardighedentrainingen ruimte in te passen om te trainen met casuïstiek met een digitale component. Te denken valt aan onderzoeken aan een plaats delict en het uitvoeren van een huiszoeking. Daarnaast is het aan te bevelen om casuïstiek te delen en tijdens kennisdagen te oefenen met succesvol afgesloten onderzoeken op het gebied van digitale criminaliteit.

6. Resumé

Op basis van de onderzoeksresultaten kan worden geconcludeerd dat er verschillen zijn waar te nemen tussen beide populaties, maar dat deze verschillen uitsluitend zijn gevonden met betrekking tot de sterkte van de gedragsintentie, alsmede de daarmee volgens de TPB en het TAM verband houdende voorspellers. Tussen de groepen onderling is er geen verschil gemeten wat betreft het daadwerkelijk gebruik van digitale sporen in de experimentele setting. De groep die wel een cursus had gevolgd en naar verwachting een hoger daadwerkelijk gebruik van digitale sporen zou tentoonspreiden, liet dit niet zien. Hiermee is een grote kloof gemeten tussen de gedragsintentie tot het gebruiken van digitale sporen in opsporingsonderzoeken en het daadwerkelijk benutten daarvan, zoals dit in het experiment is gemeten. Op basis van de TPB en het TAM is een hoge intentie tot het beoogde gedrag een goede voorspeller dat het gedrag ook daadwerkelijk wordt uitgevoerd. Een opsporingsambtenaar met een sterke gedragsintentie om gebruik te maken van digitale sporen zal dat blijkens deze theorieën ook eerder daadwerkelijk doen. Dat is in dit onderzoek echter niet aangetoond.

Uit een meervoudige regressieanalyse blijken de voorspellers die in het conceptueel model zijn opgenomen de gedragsintentie in sterke mate te kunnen voorspellen. Toch blijkt het in dit deelonderzoek opgestelde conceptueel model de gedragsintentie nauwelijks beter te voorspellen dan de concepten uit de TPB. De gepercipieerde gedragscontrole en de subjectieve norm zijn daarbij als significante voorspellers gemeten. Uit de toetsing van de hypothesen bleek dat de groep die een cursus had gevolgd een hogere score rapporteerde op deze twee voorspellers. Het volgen van een cursus op het digitale vlak hangt dus samen met het in hogere mate rapporteren dat zij zichzelf beter in staat achten om met digitale sporen te werken ten opzichte van de andere groep. Toch werd het daadwerkelijk gebruik niet verhoogd.

De maatregelen die in de politiepraktijk genomen kunnen worden om de gedragsintentie van opsporingsambtenaren tot het gebruiken van digitale sporen te verhogen zouden volgens de uitkomsten van dit onderzoek vooral in moeten grijpen op het verhogen van de gepercipieerde gedragscontrole van de individuele opsporingsambtenaar en de perceptie van de norm zoals deze volgens de opsporingsambtenaar leeft op de werkvloer. Nu de gedragsintentie een noodzakelijke voorwaarde is om te komen tot

gedragsverandering, kunnen interventies hierop als nuttig worden beschouwd, ook al is in dit onderzoek een intentie-gedragkloof gemeten. De intentie-gedragkloof kan volgens de literatuur aan de hand van implementatie-intentie worden overbrugd.

Literatuur

Aink, J.R.J. (2019). *Benutten digitale sporen: Een onderzoek naar het effect van cursussen op het benutten van digitale sporen door politiemedewerkers werkzaam binnen de opsporing.* Apeldoorn: Politieacademie (bachelor scriptie).

Ajzen, I. (1985). *From Intentions to actions: A theory of planned behavior.* In J. Kuhl & J. Beckmann (Eds), Action Control: From cognition to behavior. Berlin, Heidelber, New York: Springer-Verlag (pp. 11-39).

Armitage, C.J. & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology*, 40, 471-499.

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13, 319-339.

Gollwitzer, P.M. (1999). Implementation intentions: Strong effects of simple plans. *American Psychologist*, 54, 493-503.

Henseler, J. (2017). *De (r)evolutie van digitaal bewijs*. Leiden: Hogeschool Leiden (lectorale rede).

Holland, R.W., Aarts, H. & Langendam, D. (2006). Breaking and creating habits on the working floor: A field-experiment on the power of implementation intentions. *Journal of Experimental Social Psychology*, 42(6), 776-783.

Van Diepen, N.M., Stefanova, E. & Miranowicz, M. (2009). *Mastering skills using ICT: An active learning approach*. In A. Méndez-Vilas, A. Solano Martin, J. Mesa González & J.A. Mesa Gonzalez (Eds). Research, reflections an innovations in integrating ICT in education. Badajoz, Spain.

Webb, T.L. & Sheeran, P. (2008). Mechanisms of implementation intention effects: The role of goal intentions, self-efficacy, and accessibility of plan components. *British Journal of Social Psychology*, 47, 373-395.

Leden Redactieraad Programma Politie & Wetenschap

Uitgaven in de reeks Politiekunde

1. ***Criminaliteit in de virtuele ruimte***

   P. van Amersfoort, L. Smit & M. Rietveld, DSP-groep, Amsterdam/ TNO-FEL, Den Haag 2002

2. ***Cameratoezicht. Goed bekeken?***

   I. van Leiden & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem 2002

3. ***De 10 stappen van Publiek-Private Samenwerking (PPS)***

   J.C. Wever, A.A. van Pel & L. Smit, DSP-groep, Amsterdam/TNO-FEL, Den Haag 2002

4. ***De opbrengst van projecten. Een verkennend onderzoek naar de bijdrage van projecten aan diefstalbestrijding***

   C.J.E. In 't Velt, e.a., NPA-Onderzoeksgroep, LSOP, Apeldoorn 2003

5. ***Cameratoezicht. De menselijke factor***

   A.Weitenberg, E. Jansen, I. van Leiden, J. Kerstholt & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem/TNO, Soesterberg 2003

6. ***Jeugdgroepen in beeld. Stappenplan en randvoorwaarden voor de shortlistmethodiek***

   H.B. Ferwerda & A. Kloosterman, Advies- en Onderzoeksgroep Beke & Politieregio Gelderland-Midden, Arnhem 2004 (vierde druk 2006)

7. ***Hooligans in beeld.Van informatie naar aanpak***

   H.B. Ferwerda & O. Adang, Advies- en Onderzoeksgroep Beke, Arnhem/ Onderzoeksgroep Politieacademie Apeldoorn, 2005

8. ***Richtlijnen auditieve confrontatie***

   J.H. Kerstholt, A.G. van Amelsfoort, E.J.M. Jansen & A.P.A. Broeders, TNO Defensie en Veiligheid, Soesterberg/Politieacademie, Apeldoorn/ NFI, Den Haag 2005

9. ***Niet verschenen***

10. ***De opsporingsfunctie binnen de gebiedsgebonden politiezorg***

    O. Zoomer, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2006

11. Inzoomen en uitzoomen op Zaandam

I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem 2006

12. Aansprakelijkheidsmanagement politie. Beschrijving, analyse en handreiking

E.R. Muller, J.E.M. Polak, C.J.J.M. Stoker m.m.v. M.L. Diepenhorst & S.H.E. Janssen, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag/Faculteit der Rechtsgeleerdheid Universiteit Leiden, 2006

13. Cold cases – een hot issue

I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem 2006

14. Adrenaline en reflectie. Hoe leren politiemensen op de werkplek?

A. Beerepoot & G. Walraven e.a., DSP-groep BV, Amsterdam/Walraven onderzoek en advies, 2007

15. Tussen aangifte en zaak. Een referentiekader voor het aangifteproces

W. Landman, L.A.J. Schoenmakers & F. van der Laan, Twynstra Gudde, adviseurs en managers, Amersfoort 2007

16. Baat bij de politie. Een onderzoek naar de opbrengsten voor burgers van het optreden van de politie

M. Goderie & B. Tierolf, m.m.v. H. Boutellier & F. Dekker, Verwey-Jonker Instituut, Utrecht 2008

17. Hoeveel wordt het vandaag? Een studie naar de kans op voetbalgeweld en het veiligheidsbeleid bij voetbalwedstrijden

E.J. van der Torre, R.F.J. Spaaij & E.D. Cachet, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag 2008

18. Overbelast? De administratieve belasting van politiemensen bij de afhandeling van jeugdzaken

G. Brummelkamp & M. Linssen, EIM, Zoetermeer 2008

19. Geografische daderprofilering. Een inventarisatie van randvoorwaarden en succesfactoren

G. te Brake & A. Eikelboom, TNO Defensie en Veiligheid, Soesterberg 2008

20. Solosurveillance. Kosten en baten

S.H. Esselink, J. Broekhuizen & F.M.H.M. Driessen, Bureau Driessen, 2009

21. Onderzoek naar de mogelijke meerwaarde van AWARE voor de politie. Ervaringen met een nieuwe aanpak van belaging door ex-partners

M.Y. Bruinsma, J. van Haaf, R. Römkens & L. Balogh, IVA Beleidsonderzoek en Advies, i.s.m. INTERVICT/Universiteit van Tilburg, 2008

22. Gebiedsscan criminaliteit en overlast. Een methodiekbeschrijving

B. Beke, E. Klein Hofmeijer & P. Versteegh, Bureau Beke, Arnhem 2008

23. Informatiemanagement binnen de politie. Van praktijk tot normatief kader

V. Bekkers, M. Thaens, G. van Straten & P. Siep; m.m.v. A. Dijkshoorn, Center for Public Innovation, Erasmus Universiteit Rotterdam, 2009

24. Nodale praktijken. Empirisch onderzoek naar het nodale politieconcept

H.B Ferwerda, E.J van der Torre & V. van Bolhuis, Bureau Beke, Arnhem/ COT Instituut voor Veiligheids- en Crisismanagement, Den Haag 2009

25. Rellen om te rellen. Een studie naar grootschalige openbare-ordeverstoringen en notoire ordeverstoorders

I. van Leiden, N. Arts & H.B. Ferwerda, Bureau Beke, Arnhem 2009

26a. Verbinden van politie- en veiligheidszorg. Politie en partners over signaleren & adviseren

W. Landman, P. van Beers & F. van der Laan, Twynstra Gudde, Amersfoort 2009

26b. Politiepolitiek. Een empirisch onderzoek naar politiële signalering & advisering

E.J.A. Bervoets, E.J. van der Torre & J. Dobbelaar m.m.v. N. Koeman, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag 2009

27. De politie aan zet: de aanpak van veelplegers in Deventer

I. Bakker & M. Krommendijk, IPIT, Enschede 2009

28. Boven de pet? Een onderzoek naar grootschalige ordehandhaving in Nederland

O.M.J. Adang (redactie), S.E. Bierman, K. Jagernath-Vermeulen, A. Melsen, M.C.J. Nogarede & W.A.J. van Oorschot, Politieacademie, Apeldoorn 2009

29. Rellen in Ondiep. Ontstaan en afhandeling van grootschalige ordeverstoring in een Utrechtse achterstandswijk

G.J.M. van den Brink, M.Y. Bruinsma (redactie), L.J. de Graaf, M.J. van Hulst, M.P.C.M. Jochoms, M. van de Klomp, S.R.F. Mali, H. Quint, M. Siesling, G.H. Vogel, Politieacademie, Apeldoorn 2010

30. ***Burgerparticipatie in de opsporing. Een onderzoek naar aard, werkwijzen en opbrengsten***

A. Cornelissens & H. Ferwerda (redactie), met medewerking van I. van Leiden, N. Arts & T. van Ham, Bureau Beke, Arnhem 2010

31. ***Poortwachters van de politie. Meldkamers in dagelijks perspectief***

J. Kuppens, E.J.A. Bervoets & H. Ferwerda, Bureau Beke, Arnhem & COT, Den Haag 2010

32. ***Het integriteitsbeleid van de Nederlandse politie: wat er is en wat ertoe doet***

M.H.M. van Tankeren, Onderzoeksgroep Integriteit van Bestuur, Vrije Universiteit Amsterdam 2010

33. ***Civiele politie op vredesmissie. Uitzendervaringen van Nederlandse politie - functionarissen***

H. Sollie, Universiteit Twente, Enschede 2010

34. ***Ten strijde tegen overlast. Jongerenoverlast op straat: is de Engelse aanpak geschikt voor Nederland?***

M.L. Koemans, Universteit Leiden, 2010

35. ***Het districtelijk opsporingsproces; de black box geopend***

R.M. Kouwenhoven, R.J. Morée &. P. van Beers, Twynstra Gudde, Amersfoort 2010

36. ***Balanceren tussen alert maken en onrust voorkomen. Publiekscommunicatie over seriële schokkende incidenten (casestudy Lelystad)***

A.J.E. van Hoek, m.m.v. P.F. van Soomeren, M.D. Abraham & J. de Kleuver, DSP-groep, Amsterdam 2011

37. ***Sturing van blauw. Een onderzoek naar operationele sturing in de basispolitiezorg***

W. Landman, m.m.v. M. Malipaard, Twynstra Gudde, Amersfoort 2011

38. ***Onder het oppervlak. Een onderzoek naar ontwikkelingen en (a)select optreden rond preventief fouilleren***

J. Kuppens, B. Bremmers, E. van den Brink, K. Ammerlaan & H.B. Ferwerda, m.m.v. E.J. van der Torre, Bureau Beke, Arnhem/COT, Den Haag 2011

39. ***Naar eigen inzicht? Een onderzoek naar beoordelingsruimte van en grenzen aan de identiteitscontrole***

J. Kuppens, B. Bremmers, K. Ammerlaan & E. van den Brink, Bureau Beke, Arnhem/COT, Den Haag 2011

40. Toezicht op zedendelinquenten door de politie in samenwerking met de reclassering

H.G. van de Bunt, N.L. Holvast & J. Plaisier, Erasmus Universiteit, Rotterdam/Impact R&D, Amsterdam 2012

41. Daders over cameratoezicht

H.G.A. van Schijndel, A. Schreijenberg, G.H.J. Homburg & S. Dekkers, Regioplan Beleidsonderzoek, Amsterdam 2012

42. Aanspreken op straat. Het werk van de straatcoach in al zijn verschijnings - vormen

L. Loef, K. Schaafsma & N. Hilhorst, DSP-groep, Amsterdam 2012

43. De organisatie van de opsporing van cybercrime door de Nederlandse politie

N. Struiksma, C.N.J. de Vey Mestdagh & H.B. Winter, Pro Facto, Groningen/ Kees de Vey Mestdagh, Groningen 2012

44. Politie in de netwerksamenleving. De opbrengst van de politiële netwerkfunctie voor de kerntaken opsporing en handhaving openbare orde en de sturing hierop in de gebiedsgebonden politiezorg

I. Helsloot, J. Groenendaal & E.C. Warners, Crisislab, Renswoude 2012

45. Tegenspraak in de opsporing. Verslag van een onderzoek

R. Salet & J.B. Terpstra, Radboud Universiteit Nijmegen 2012

46. Tunnelvisie op tunnelvisie? Een verkennend en experimenteel onderzoek naar de besluitvorming door VKL-teams met betrekking tot het onderkennen van tunnelvisie en andere procesaspecten

I. Helsloot, J. Groenendaal & B. van 't Padje, Crisislab, Renswoude 2012

47. M.-waarde. Een onderzoek naar de bijdrage van Meld Misdaad Anoniem aan de politionele opsporing

M.C. van Kuik, S. Boes, N. Kop, M. den Hengst-Bruggeling, T. van Ham & H. Ferwerda, Politieacademie, Apeldoorn/Bureau Beke, Arnhem 2012

48. Seriebrandstichters. Een verkennend onderzoek naar daderkenmerken en delictpatronen

Y. Schoenmakers, A. van Wijk & T. van Ham, Bureau Beke, Arnhem 2012

49. Van wie is de straat? Methodiek en lessen voor de politie om ongrijpbare veiligheidsfenomenen grijpbaar te maken – op basis van vijf praktijkcasus

H. Ferwerda, T. van Ham, B. Bremmers, K. Tijhof & M. Grotens, Bureau Beke, Arnhem 2013

50. ***Recherchesamenwerking in de Euregio Maas-Rijn. Knooppunten, knelpunten en kansen***

H. Nelen, M. Peters & M. Vanderhallen, Politieacademie, Apeldoorn/ Universiteit Maastricht 2013

51. ***De operationele politiebriefing onderzocht. Een onderzoek naar de effectiviteit van de operationele politiebriefing***

A. Scholtens, J. Groenendaal & I. Helsloot, Crisislab, Renswoude 2013

51a. ***De operationele politiebriefing onderzocht (2). Een actie(vervolg) onderzoek om tot een effectievere politiebriefing te komen***

A. Scholtens, Crisislab, Renswoude 2015

52. ***Sociale media: factor van invloed op onrustsituaties?***

R.H. Johannink, I. Gorissen & N.K. van As, Politieacademie Apeldoorn/ VDMMP, Houten 2013

53. ***De terugkeer van zedendelinquenten in de wijk***

C.E. Huls & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen/Centrum voor Openbare Orde en Veiligheid, Groningen 2013

54. ***Van meld- naar aantoonplicht. Een onderzoek naar een systeem van digitale surveillance***

C. Veen & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen 2013

55. ***Heterdaadkracht in twee Haagse pilotgebieden***

B. van Dijk, J.B. Terpstra & P. Hulshof, Politieacademie, Apeldoorn/ DSPgroep, Amsterdam 2013

56. ***Inzet op Maat. Onderzoek naar kenmerken en mogelijkheden van duurzame inzetbaarheid van oudere medewerkers***

H. de Blouw, I.R. Kolkhuis Tanke & C.C. Sprenger, Politieacademie, Apeldoorn 2013

57. ***Interventies in de opsporing. Impulsen in kwaliteit en effectiviteit van het opsporingsproces***

R.M. Kouwenhoven, R.J. Morée & P. van Beers, Twynstra Gudde, Amersfoort 2013

58. ***De plaats delict in beeld. Fotografie in de dagelijkse en gesimuleerde praktijk***

G. Vanderveen & J. Roosma, Instituut voor Strafrecht & Criminologie, Universiteit Leiden 2013

59. Jeugdgroepen van toen. Een casusonderzoek naar de leden van drie criminele jeugdgroepen uit het einde van de vorige eeuw

H. Ferwerda, B. Beke & E. Bervoets, Bureau Beke, Arnhem/Beke Advies, Arnhem/LokaleZaken, Rotterdam 2013

60. Tussen hei en hoofdbureau. Leiderschapsontwikkeling bij de politie

W. Landman, M. Brussen & F. van der Laan, Twynstra Gudde, Amersfoort 2013

61. Gemeentelijk blauw. Het dagelijks werk van gemeentelijke handhavers in beeld

E. Bervoets, J. Bik & M. de Groot, LokaleZaken, Rotterdam 2013

62. Excessief geweld op en om de voetbalvelden. Praktijkonderzoek naar omvang, ernst en aanpak van 'voetbalgeweld'

P. Duijvestijn, B. van Dijk, P. van Egmond, M. de Groot, D. van Sommeren & A. Verwest, DSP-groep, Amsterdam 2013

63. Beeld van gezag bij de politie. Maatschappelijke verbeelding en de impact van gezagsbeelden op burgers

H. de Mare, B. Mali, M. Bleecke & G. van den Brink, m.m.v. Motivaction, Tilburg University, Stichting IVMV, Leiden 2014

64. Informatiegestuurde dienders. Informatiesturing tussen theorie en praktijk

A. van Sluis, P. Siep, V. Bekkers, m.m.v. M. Thaens & G. Straten, Center for Public Innovation, Erasmus Universiteit, Rotterdam 2014

65. Hard op weg. Onderzoek aanpak verkeersveelplegers

B. Bieleman, M. Boendermaker, R. Mennes & J. Snippe, Intraval, Groningen/Rotterdam 2014

66. Tussen hulp en hype. De inzet van opsporingsberichtgeving in ontvoeringszaken

Y.M.M. Schoenmakers, J.V.O.R. Doekhie & J.C. Knotter, Yvette Schoenmakers Onderzoek en advies, Weesp 2014

67. Nachtdienst bij de politie en verkeersveiligheid. Onderzoek naar ervaringen van politieagenten met verkeersonveiligheid in woon-werkverkeer na de nachtdienst

P. Boekhoorn, BBSO, Nijmegen 2014

68. Buit van woninginbraak. Onderzoek onder inbrekers en helers

J. Snippe, M. Sijtstra, R. Mennes & B. Bieleman, Intraval, Groningen/Rotterdam 2014

69. ***Privaat blauw. Portiers, evenementbeveiligers en voetbalstewards op risicovolle locaties en tijdens risicovolle momenten***

E. Bervoets & S. Eijgenraam, LokaleZaken, Rotterdam 2014

70. ***Met grof geschut. Reconstructie van een moordonderzoek binnen de criminele woonwagenwereld***

I. van Leiden, B. Bremmers & H. Ferwerda, Bureau Beke, Arnhem 2014

71. ***Met fluwelen handschoenen? Politie en de omgang met verwarde personen in Amsterdam***

J. Kuppens, T. Appelman, T. van Ham & A. van Wijk, Bureau Beke, Arnhem 2015

72a. ***Vermisten op de kaart. Aard en omvang van langdurige vermissingen***

I. van Leiden & M. Hardeman, Bureau Beke, Arnhem 2015

73. ***Van intel tot operatie. De impact van veiligheidsanalisten bij de aanpak van misdaad***

M. den Hengst, M. Bruinsma, Y. Schoenmakers, W. Niepce, Bureau Bruinsma, Tilburg 2015

74. ***De bestuurlijke rapportage. Gezamenlijke inspanning in de aanpak van (georganiseerde) criminaliteit en overlast***

I. Gorissen, m.m.v. R.H. Johannink, PBLQ, Den Haag 2015

75. ***De aangifte van delicten bij de multichannelstrategie van de politie***

P. Boekhoorn & J. Tolsma, Bureau Boekhoorn/Radboud Universiteit, Nijmegen 2016

76. ***Die pakken we toch niet op? Afstemming tussen politie en Openbaar Ministerie in zaken van veelvoorkomende aangiftecriminaliteit***

R. Kouwenhoven & L. Kleijer-Kool, Twynstra Gudde, Amersfoort 2016

77. ***Het real-time informeren van noodhulpeenheden. Een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie***

A. Scholtens, M. den Hengst & R. Waterreus, Crisislab, Renswoude/ Politieacademie, Apeldoorn 2016

78. ***Hoe lang kun je 'schijt hebben'? Dertien desisters uit criminele jeugdgroepen aan het woord***

C.E. Hoogeveen, A.E. van Burik & B.J. de Jong, m.m.v. E.M. Klooster, Bureau Alpha, 's-Hertogenbosch/VanMontfoort, Woerden 2016

79. ***Onbenutte kansen. Een onderzoek naar het gebruik van restinformatie in de opsporing***

A. van Wijk & L. Scholten, m.m.v. B. Bremmers, Bureau Beke, Arnhem 2016

80. ***Verbale leugendetectie-wizards***

G. Bogaard & E.H. Meijer, Maastricht University, Maastricht 2016

81. ***Mensenhandel in de prostitutie opsporen zonder aangifte? Een vervolgonderzoek om de doorzettingsmacht van de politie te verduidelijken***

M. Goderie, m.m.v. R. Kool, Goderie Onderzoek, Klarenbeek 2016

82. ***De onvindbaren. Op zoek naar voortvluchtige veroordeelden in Nederland***

Y. Schoenmakers, I. de Groot, J. van Zanten, A. van Rooyen & J. Baars, Yvette Schoenmakers onderzoek & advies, Amsterdam 2017

83. ***Elke dump is een plaats delict. Dumping en lozing van synthetisch drugsafval: verschijningsvormen en politieaanpak***

Y. Schoenmakers, S. Mehlbaum, M. Everartz & C. Poelarends, Yvette Schoenmakers onderzoek & advies, Amsterdam 2016

83A. ***De Intelligence Paradox. Lessen uit de integrale pilot Analyse Synthetische***
Drugs in Oost-Nederland

Y. Schoenmakers, S. Mehlbaum, Yvette Schoenmakers onderzoek & advies, Amsterdam 2019

84. ***Naar handhaafbare noodbevelen en noodverordeningen. Een analyse van het gemeentelijke noodrecht***

A.J. Wierenga, C. Post & J. Koornstra, Rijksuniversiteit Groningen, Centrum voor Openbare Orde en Veiligheid, 2016

85. ***Vermisten op het spoor. Rechercheren naar langdurige vermissingen***

I. van Leiden & M. Hardeman, Bureau Beke, Arnhem 2017

86. ***De aard van het beestje. Kenmerken en achtergronden van dierenmishandelaars***

A. van Wijk & M. Hardeman, Bureau Beke, Arnhem 2017

87. ***Modus operandi van de recherche. De rechercheprakijk in moord- en verkrachtingszaken***

A. van Wijk, I. van Leiden & M. Hardeman, Bureau Beke, Arnhem 2017

88. ***Over grenzen in de sport. De rol van de politie in de aanpak van seksueel grensoverschrijdend gedrag in de sport in samenwerking met relevante partners***

A. van Wijk, M. Hardeman, L. Scholten & M. Olfers, Vrije Universiteit Amsterdam, Bureau Beke, Arnhem 2017

89. ***Defensiehulp. Legergroene bijstand aan de politie bij handhaving van de rechtsorde***

E. Bervoets, m.m.v. S. Eijgenraam, T. Dijkhuizen & J. van de Werken, Bureau Bervoets, Amersfoort 2017

90. ***Tussen onder en boven. Productie en distributie van softdrugs in Noord- Nederland***

J. Snippe, R. Mennes, M. Sijtstra & B. Bieleman, Intraval, Groningen/ Rotterdam 2017

91. ***Vechten op afspraak. Inzicht in het fenomeen en input voor de ontwikkeling van een politiestrategie***

T. van Ham, L. Scholten, A. Lenders & H. Ferwerda, Bureau Beke, Arnhem 2018

92. ***Notoire straten. Over de lokale inbedding van georganiseerde criminaliteit***

S. Mehlbaum, Y. Schoenmakers & J. van Zanten, Mehlbaum Onderzoek, Amsterdam 2018

92A. ***De wortel en de stok. Praktijklessen uit een gebiedsgerichte probleemaanpak van ondermijning***

S. Mehlbaum, Y. Schoenmakers, Mehlbaum Onderzoek, Amsterdam 2019

93. ***Ondermijning door criminele 'weldoeners'***

M. Bruinsma, R. Ceulen & T. Spapens, m.m.v. C. Deij, Tilburg University, Tilburg/Bureau Bruinsma, Tilburg 2018

94. ***Kiezen voor politie. Een onderzoek onder mbo-studenten met een migratie - achtergrond in het veiligheidsdomein***

S. de Winter-Koçak, E. Klooster & M. Day, m.m.v. S. Mehlbaum, M. van Vugt & K. Leschonski, Verwey-Jonker Instituut, Utrecht 2018

95. ***Doe-het-zelf-surveillance. Een onderzoek naar de werking en effecten van WhatsApp-buurtgroepen***

S. Mehlbaum & R. van Steden, m.m.v. M. van Dijk, Vrije Universiteit Amsterdam, Mehlbaum Onderzoek, Amsterdam 2018

96. ***Een klacht is een gratis advies***

G. Jacobs, T. Hak, G. Vanderveen, M. Flory, T. Thuis, S. Valkeman & M. Franken, Erasmus Universiteit, Rotterdam 2018

97. ***Voortgezet crimineel handelen tijdens detentie: je gaat het pas zien als je het doorhebt***

A. Verwest, W. Buysse, P. van Egmond, D. Hofstra, DSP-groep, Amsterdam 2019

98. ***Zorg voor kinderen bij aanhouding van ouders; Best practices uit binnen- en buitenland***

J. Reef, N. Ormskerk, Universiteit Leiden 2019

99. ***Aankoopfraude uit het buitenland***

J. Jansen, S. Westers, S. Twickler, W. Stol, NHL Stenden Hogeschool / Politieacademie

100. ***Grijs vakmanschap? Taakgerelateerd ongeoorloofd handelen binnen de politie***

R. Chr. van Halderen (diss. Avans Hogeschool), 2019

101. ***Niet meer doen! Een onderzoek naar de INDIGO-afdoening***

A. van Wijk, S. Dickie, J. van Esseveldt, Bureau Beke, Arnhem 2019

102 ***De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging***

P. Boekhoorn, BBSO, Nijmegen 2020

103 ***In- en doorstroom van nieuwkomers in beeld. Opgetekende lessen uit acht casussen rond de opvang van asielzoekers in Nederland***

J. Kuppens, Bureau Beke, Arnhem 2020

104 ***De lading van vuurwapens. Een onderzoek naar de impact van illegale vuurwapens in Nederland***

H. Ferwerda, J. Wolsink en I. van Leiden, Bureau Beke, Arnhem 2020

105 ***Q-teams. De politie onderweg naar toekomstbestendige opsporing en vervolging?***

P. van Egmond, A. Swami-Persaud, A. Verwest, DSP-groep, Amsterdam 2020

106 ***Onderwereld boven water? Zoektocht naar georganiseerde criminaliteit in de Noordelijke zeehavens***

N. Struiksma, C. Boxum, S.J. Hollenberg, N.O.M. Woestenburg, Pro Facto, Groningen 2020