Amsterdam University of Applied Sciences

Digitale sporen in smartphones. Een kennismaking met pattern-of-life forensics

Author(s)
Meconi, Timo; Henseler, Hans

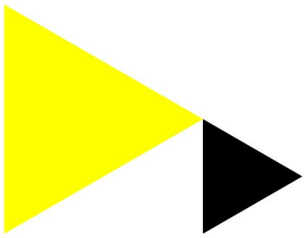
Publication date
2022

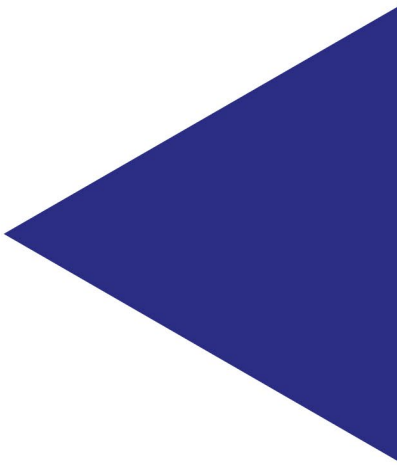
Document Version
Final published version

Published in
Expertise en Recht

Link to publication

Citation for published version (APA):
Meconi, T., & Henseler, H. (2022). Digitale sporen in smartphones. Een kennismaking met *pattern-of-life forensics*. *Expertise en Recht*, *2022*(3), 70-77. https://www.uitgeverijparis.nl/nl/reader/210952/1001620247





General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please contact the library: https://www.amsterdamuas.com/library/contact/questions, or send a letter to: University Library (Library of the University of Amsterdam and Amsterdam University of Applied Sciences), Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

Creating Tomorrow

Download date:13 Oct 2024

Timo Meconi en Hans Henseler***

Digitale sporen in smartphones. Een kennismaking met *pattern-of-life forensics*[1]

Mensen laten in het dagelijks leven steeds meer digitale sporen achter in computers, tablets en smartphones die waardevol kunnen zijn voor de opsporing en voor de bewijsvoering in strafzaken. Naast sporen die we bewust achterlaten, zoals berichten, foto's en video's, laten onze handelingen ook allerlei sporen na waarvan we ons veelal niet bewust zijn. Tezamen bieden al deze sporen een kijkje in het dagelijks activiteitenpatroon van een gebruiker. Het digitaal forensisch onderzoek dat zich hierop richt, wordt aangeduid als pattern-of-life forensics. Dit onderzoek is een waardevolle aanvulling voor het toetsen en opstellen van scenario's, maar tegelijkertijd is het ook een complex onderzoeksgebied vanwege de snelle ontwikkelingen in hardware en software.
In dit artikel geven we een aantal voorbeelden van pattern-of-life forensics aan de hand van rechterlijke uitspraken, experimenten die zijn uitgevoerd met smartphones en onderzoek dat is gepubliceerd in de literatuur. In het bijzonder hebben we ons daarbij gericht op het aantonen of een handeling met voorbedachte raad is verricht, op het aantonen van eigenaarschap van een smartphone en op de betrouwbaarheid van digitale sporen als die worden betwist. Juist het dagelijkse patroon van activiteiten dat door middel van pattern-of-life forensics wordt vastgesteld, kan bij uitstek vergeleken worden met observaties uit andere bronnen zoals beveiligingscamera's, andere inbeslaggenomen bewijsstukken en/of getuigenverklaringen.

1. Inleiding

Het onderzoeken van smartphones biedt een goudmijn aan informatie voor de opsporingsdiensten. Een gemiddelde smartphone houdt tegenwoordig meer bij dan alleen foto's, video's en chatgesprekken. Voor veel mensen is het een essentieel onderdeel van hun leven. Tel bijvoorbeeld het aantal oplichtende schermen in het openbaar vervoer of in wachtruimtes. Dit fenomeen is een logisch gevolg van de digitalisering van de samenleving. Steeds meer diensten worden immers aangeboden via applicaties of websites. Wat veel gebruikers zich niet realiseren, is dat de data op een smartphone worden verzameld en opgeslagen. Ook rechercheurs zijn hier niet altijd alert op en missen hierdoor mogelijkheden die van belang kunnen zijn voor het opsporingsonderzoek.

Digitale sporen bieden namelijk, in tegenstelling tot fysieke sporen, vaak precieze tijden met daaraan gekoppeld activiteiten. In combinatie met de zeven W-vragen geven dit soort sporen meer informatie rondom een bepaalde gebeurtenis. Deze vragen beginnen met wie, wat, waar, waarmee, op welke wijze, wanneer en waarom. Antwoorden op deze vragen helpen bij het maken van een reconstructie van strafrechtelijk relevante gebeurtenissen.[2, 3] Met name handelingen die een gebruiker (on)bewust uitvoert, laten sporen achter die waardevol zijn voor het maken van een reconstructie of toetsen van een scenario. Het onderzoek naar afzonderlijke sporen kan ook worden uitgebreid met onderzoek naar relaties tussen digitale sporen onderling. Door verschillende activiteiten met elkaar te koppelen, kunnen specifieke scenario's worden getoetst. In het Engels worden dit soort sporen *pattern-of-life*-sporen genoemd en het digitaal forensisch onderzoek *pattern-of-life forensics*.[4] Deze patronen beperken zich niet alleen tot de stappenteller in een smartphone. Een smartwatch heeft bijvoorbeeld de functie die met behulp van een sensor de hartslag van de drager monitort. In theorie zou een overlijden of een tijdstip van overlijden aan de hand van de hartslag kunnen worden vastgesteld.

Het gebruik van *pattern-of-life*-sporen geeft de opsporing mogelijkheden om specifieke scenario's te toetsen. *Pattern-of-life*-sporen kunnen echter niet zonder meer als bewijs worden gebruikt. Deskundigen dienen dit soort sporen in de context van de zaak te plaatsen. Dat kan aan de hand van zaaksinformatie, maar dit is niet altijd nodig. Met *pattern-of-life*-sporen kan een digitaal rechercheur of expert ook individuele onderdelen van een scenario toetsen. Centraal staan hierbij de volgende vragen: wie is de gebruiker, zijn de te onderzoeken gedragingen opzettelijk (en met voorbedachte raad) verricht en hoe betrouwbaar zijn de data? Door deze drie vragen te beantwoorden kan een digitaal rechercheur of expert *pattern-of-life*-sporen interpreteren met minimale kennis van de zaak.

2. *Pattern-of-life forensics*

In de fysieke wereld kan *pattern-of-life* gaan om observaties van individuen of locaties. Dezelfde soort analyses kunnen met digitale gegevensdragers worden gemaakt. Met name smartphones bevatten veel mogelijkheden op dit gebied. Binnen dit artikel wordt gefocust op iPhones, omdat dit type smartphone veel data in het eigen geheugen opslaat. *Pattern-of-life* is een relatief nieuwe term

* T.N.T. Meconi BSc is docent Digitaal Forensisch Onderzoek bij de Hogeschool van Amsterdam en cyberspecial bij de Nationale Politie.

** Dr. ir. J. Henseler is lector *E-Discovery* en *Digital Forensics* bij Hogeschool Leiden, senior wetenschappelijk onderzoeker bij het Nederlands Forensisch Instituut en tevens redacteur van dit tijdschrift.

1. De auteurs bedanken mr. G. Haverkate, mr. M. Dubelaar en mr. J. Hielkema voor hun waardevolle commentaar en aanvullingen op eerdere versies van dit artikel. Ze bedanken ook het NFI voor de mogelijkheid en ondersteuning die aan de eerste auteur is gegeven om bij het NFI af te studeren op het onderzoek waarvan de resultaten zijn gebruikt in dit artikel.
2. Henseler & De Poot 2020.
3. De Poot 2011.
4. Meconi 2021.

binnen digitaal forensisch onderzoek. In plaats van het wiel opnieuw uit te vinden, kan gekeken worden bij de inlichtingenwereld. Zo gebruikten de Amerikanen *pattern-of-life* voor het inwinnen van informatie ten tijde van de Afghaanse oorlog tussen 2004 en 2007. Met behulp van dronebeelden konden analisten individuen koppelen aan gebouwen en routes in kaart brengen. Deze analyse voorafgaand aan een inval heeft zich meerdere malen bewezen als inlichtingenmiddel.[5]

De betrouwbaarheid van de registratie van bewegingen (zoals wandelbewegingen) in iPhones kent beperkingen. Dat blijkt onder andere uit een artikel over de betrouwbaarheid van de Apple Health App dat in 2019 door het Nederlands Forensisch Instituut (NFI) gepubliceerd is. Van Zandwijk en Boztas focusten zich op de healthdb_secure.sqlite-database, die onder andere het aantal stappen en de afstand opslaat. Uit hun onderzoek blijkt dat het aantal geregistreerde stappen uit de iPhone nagenoeg overeenkwam met het aantal stappen dat met een handteller was geteld. De geregistreerde afgelegde afstand is minder nauwkeurig. Het maken van overdreven armbewegingen leidde tot een langere geregistreerde afstand. Het stilhouden van de armen kwam overeen met de daadwerkelijke afstand, terwijl bij rennen een kleinere afstand werd geregistreerd. De locatie van het dragen van een iPhone in de hand beïnvloedt de geregistreerde afstand.[6] In een vervolgonderzoek in 2021 geven Van Zandwijk en Boztas aan dat de logbestanden van WhatsApp en cache_encryptedC van Apple kunnen bijhouden wat voor soort bewegingen hebben plaatsgevonden. Zo registreert zowel het WhatsApp logsysteem als een Apple database of de smartphone zich beweegt in een voertuig. De auteurs/onderzoekers plaatsen hierbij wel de kanttekening dat digitale experts geen overhaaste conclusies uit deze gegevens moeten trekken. Zo is niet bekend hoe de data precies tot stand komen. Een aanbeveling uit het artikel is om te onderzoeken of verschillende databronnen met elkaar gecombineerd kunnen worden.[7] *Pattern-of-life forensics* ligt in het verlengde hiervan, maar focust niet alleen op de stappenteller. Een iPhone heeft ook andere databases die *pattern-of-life*-sporen bevatten. Voorbeelden hiervan zijn: registratie van de ontgrendeling van de telefoon, batterijgebruik en applicatiegebruik. Sarah Edwards en Alexis Brignoni houden een lijst bij met verschillende soorten *pattern-of-life*-sporen, die een digitaal expert kan vinden op een iPhone. Beiden publiceren dit op hun blog[8] en via Github[9], wat het mogelijk maakt om als digitaal expert zelf de computerprogramma's te valideren en eventueel aan te passen naar eigen behoefte. Door software-updates bij iOS kan het namelijk voorkomen dat deze computerprogramma's in mindere mate tot niet werken. De validatiestap helpt in het bepalen voor welke digitale sporen dit geldt. Dit artikel gaat voor de rest niet in op de technische details voor het gebruik hiervan. De kennis dat een smartphone verschillende soorten *pattern-of-life*-sporen bevat, is voldoende voor een goed begrip van de rest. In de volgende onderdelen zal het gebruik van *pattern-of-life*-sporen worden besproken aan de hand van verschillende voorbeelden.

3. Gebruik van digitale sporen

Digitale experts moeten voorzichtig zijn met het interpreteren van digitale sporen. Casey geeft aan dat de politie soms te weinig kennis heeft om digitaal onderzoek te verrichten, maar ook een kritische blik mist voor beperkingen van de methode en het oplossen van gebruikersproblemen (inladen van data of exporteren van resultaten). Dit zou kunnen leiden tot een verkeerde interpretatie van het digitale sporenbeeld.[10] De vraag is hoe het in Nederland is gesteld met de kennis op het gebied van digitale sporen. In het geval van cybercrime blijkt uit een rapport van de Cybersafety Research Group waarin onderzoek is gedaan naar het kennisniveau van politiemensen met betrekking tot de digitale aspecten van het politiewerk, dat deze kennis binnen de politie niet op het gewenste niveau ligt. De onderzoekers geven aan dat het bestrijden van dit kennistekort geen eenvoudige opgave is en doen meerdere aanbevelingen om dit te verbeteren. Ze stelden een online vragenlijst op die door 402 respondenten is ingevuld. Bij de analyse van de antwoorden richtten de onderzoekers zich op: functiegroep, geslacht, leeftijd, opleiding en ervaring. Politiemensen met opleidingen en ervaring in cybercrime blijken significant hoger te scoren dan politiemensen zonder gerichte opleiding en ervaring. Het opleiden van personeel heeft dus effect.[11]

De Nederlandse politie is zich er wel degelijk van bewust dat er digitale kansen bestaan, maar politiemensen weten deze niet altijd te benutten. Zuurveen & Stol hebben in 2020 onderzoek gedaan naar het gebruik van digitale sporen. Politiemensen zien de meerwaarde van veelvoorkomende gegevensdragers in hun onderzoeken, maar voor nieuwere gegevensdragers moeten ze nog wel een beroep doen op digitale expertise.[12] Respondenten geven verder aan dat digitale sporen niet liegen, betrouwbaar zijn en daarmee objectiever dan analoge sporen.[13] Een ander gedeelte van het onderzoek focuste zich op de keuze om digitale sporen te gebruiken. De onderzoekers maakten hiervoor een casus, waarbij tien keuzes werden voorgelegd. De respondenten hadden keuze uit een analoog of digitaal bewijsstuk. Denk hierbij aan buurtonderzoeken en verhoren als analoog bewijsstuk en uitlezen van telefoons en openbronnenonderzoek als digitaal bewijsstuk. Opmerkelijk genoeg kiezen oudere respondenten (51 jaar en ouder) vaker voor een digitaal bewijsstuk dan voor een analoog bewijsstuk dan de jongere respondenten (tot 30 jaar). Volgens de onderzoekers remt de vergrijzing dus niet het gebruik van digitale sporen.[14]

5. Flynn e.a. 2008.
6. Van Zandwijk & Boztas 2019.
7. Van Zandwijk & Boztas 2021.
8. Edwards en Brignoni.
9. Github is een online platform, waarbij programmeurs computercodes kunnen uitwisselen op het internet.
10. Casey 2019a.
11. Jansen e.a. 2020, p. 24-30 en 87-90.
12. Zuurveen & Stol 2020, p. 74.
13. Zuurveen & Stol 2020, p. 47, 73 en 91.
14. Zuurveen & Stol 2020, p. 86-88 en 91-92.

De veronderstelling dat digitale sporen betrouwbaarder zijn dan analoge sporen, is niet zonder risico. Het kan voorkomen dat digitale sporen op verschillende manieren geïnterpreteerd kunnen worden. Zo kan een expert overtuigd zijn dat de resultaten uit zijn analyse 100% betrouwbaar zijn, terwijl een andere expert twijfelt over de analysemethode en de resultaten betwist. Het is dan lastig om te bepalen welke expert gelijk heeft, wat schadelijk kan zijn voor het vertrouwen. Een ander voorbeeld is het aanpassen van een computersysteem. Hierbij wijzigt de gebruiker het systeem om specifieke bestanden of applicaties te verbergen. Als alleen wordt gefocust op de betrouwbaarheid van het computersysteem zelf of het vinden van deze bestanden, wordt voorbijgegaan aan de mogelijke sporen die indicatie geven dat de bestanden zijn verborgen door de gebruiker. Bepaalde stappen dienen gevolgd te worden om een bestand onzichtbaar te maken. Ook deze processen laten sporen na op een computer, die een digitaal expert later kan achterhalen.[15] Het vinden van een gewiste foto is niet meer voldoende, om een conclusie te trekken of de gebruiker deze zelf heeft gewist. Om een uitspraak te kunnen doen over de herkomst ervan, dient een expert verder te kijken door te achterhalen waar precies de foto was opgeslagen en welke processen rond de tijd van opslaan draaiden.

Dat de politie deze kansen ook benut in de praktijk, blijkt onder meer uit een uitspraak met betrekking tot brandstichting. De verdachte in deze zaak zou verantwoordelijk zijn voor het stichten van meerdere branden in een straat in Leeuwarden die tot grote onrust bij de buurtbewoners hadden geleid. Het onderzoek aan de telefoon van de verdachte is een goed voorbeeld van wat mogelijk is met digitale sporen. De rechtbank leidt aan de hand van de stappenteller af dat 'de telefoon iedere keer direct voorafgaand aan de respectievelijke brandmeldingen bewegingen heeft gesignaleerd over (…) afstanden die passen bij het door verdachte verlaten van zijn woning, het stichten van een brand en het weer terugkeren naar zijn woning.' In sommige gevallen was op de telefoon te zien dat de website alarmeringen.nl na de brandstichting werd bezocht.[16] Het kunnen afleiden van dit soort patronen biedt genoeg aanknopingspunten in een opsporingsonderzoek. Een stappenteller is slechts één van de mogelijkheden, maar een goed startpunt om andere digitale sporen effectief te benutten.

4. Eigenaarschap

Het koppelen van een persoon aan digitale sporen is lastiger dan bij fysieke sporen. Meerdere personen kunnen dezelfde smartphone gebruiken als ze de inlogcode weten of als de telefoon al is ontgrendeld. Biometrie zou mogelijk de uitkomst kunnen bieden om een gebruiker te identificeren. Moderne smartphones bevatten een vingerscansensor en een camera voor gezichtsherkenning. De gebruiker kan zelf kiezen welke van deze twee vormen worden toegevoegd als middel ter ontgrendeling van de smartphone. Een ander voorbeeld is het gebruiken van de vingerscan om betalingen goed te keuren via bankapplicaties.

Identificatie aan de hand van de vingerscan heeft beperkingen door het registratie- en logsysteem van de iPhone. De iPhone kan maximaal vijf vingerafdrukken opslaan. Tijdens het registreren plaatst de gebruiker zijn/haar vinger op de scan. Door de vinger te roteren scant de smartphone de papillairlijnen. Het staat de gebruiker vrij om ook andere vingers op de scan te leggen in plaats van dezelfde vinger te scannen. Hierdoor is het mogelijk dat de smartphone tot wel drie vingers opslaat voor één afdruk. In de praktijk betekent dit dat alledrie de vingerafdrukken geldig zijn, om de smartphone te kunnen ontgrendelen. Daarbij speelt ook het probleem dat iPhone de inlogpogingen niet afzonderlijk van elkaar bijhoudt, waardoor wel kan worden vastgesteld dat op de iPhone is ingelogd met een vingerafdruk maar niet het exacte tijdstip daarvan. In het logbestand ADDataStore.sqlitedb telt de iPhone het aantal inlogpogingen voor de afdrukken, hetgeen inzicht kan geven of de gebruiker de telefoon met behulp van een vingerafdruk wilde ontgrendelen.

Eigenaarschap kan ook bepaald worden door handelingen van de gebruiker te analyseren aan de hand van activiteiten. Het combineren van sporen uit een iPhone en Apple smartwatch kan inzicht geven in het gedragspatroon van de gebruiker. Het voordeel is dat een Apple smartwatch de gegevens opslaat op de iPhone. Hierdoor is een aparte extractie van de smartwatch niet nodig. Uiteraard mag onderzoek in de smartphone waarbij de telefoon wordt uitgelezen alleen plaatsvinden met toestemming van een rechter-commissaris, omdat veelal te voorzien is dat de inbreuk op de persoonlijke levenssfeer van de gebruiker zeer ingrijpend zal zijn.[17] Echter, voor het toetsen van bepaalde scenario-elementen zou een *pattern-of-life*-analyse van toegevoegde waarde kunnen zijn voor het onderzoek.

Data uit verschillende gegevensdragers met elkaar vergelijken, is een andere mogelijkheid om specifieke handelingen toe te wijzen aan verdachten. Bij een moord stelde de politie camerabeelden veilig met daarop de twee mogelijke daders. Beiden waren in het zwart gekleed, waardoor het lastig was om duidelijke persoonlijke kenmerken te onderscheiden. Een getuige wees één van de daders aan als schutter en de ander als chauffeur. Een van de twee werd snel na het delict aangehouden. Een groot voordeel was dat de telefoon die bij hem in beslag genomen werd, snel is uitgelezen, waardoor de cache-bestanden[18] beschikbaar waren. De politie kon de gegevens op de telefoon vergelijken met de camerabeelden. De smartphone van de chauffeur registreert dat deze zich in een voertuig bevindt en beweegt voor 15:22:38 uur. Op een camera is te zien dat de schutter instapt bij de chauffeur rond 15:22:38 uur. Op 15:22:39 uur is een registratie te zien dat de smartphone niet beweegt. Rond 15:22:45 uur registreert de smartphone weer beweging. Op de camerabeelden rijdt de auto op 15:22:46 uur weg.

15. Casey 2019b.
16. Rb. Noord-Nederland 10 juli 2020, ECLI:NL:RBNNE:2020:2633.
17. HR 4 april 2017, ECLI:NL:HR:2017:584, *NJ* 2017/229, m.nt. T. Kooijmans.
18. De term 'cache' is een veelgebruikte computerterm om een tijdelijke opslagplaats (in dit geval een bestand) aan te duiden waarin gegevens tijdelijk worden opgeslagen zodat de omvang van het bestand beperkt blijft.

Op basis van de gegevens van de smartphone is niet te zeggen of de verdachte de rol van chauffeur of overvaller had. Dat de verdachte een rol had in deze zaak, is wel aannemelijker. Al moet wel blijken uit andere (niet-) digitale sporen of de verdachte überhaupt de 'hoofdgebruiker' is. Welke gebruikersnamen komen overeen met benamingen van de verdachte? Op welke foto's staat de verdachte? Welke locaties of zendmastgegevens zijn terug te vinden?

Door deze vragen te beantwoorden, ontstaat een beter beeld of de verdachte de hoofdgebruiker van de telefoon is. Zo stelde het NFI in 2017 een interdisciplinair rapport op in het kader van een Interdisciplinair Forensisch Onderzoek (IDFO), om de gebruiker van een tipgevertelefoon te achterhalen. De verdachte gebruikte deze telefoon om de locatie van het slachtoffer aan de schutter door te geven. Het NFI maakte gebruik van resultaten uit drie onafhankelijke deelonderzoeken: Automatic Number Plate Recognition (ANPR-gegevens)[19], telecomgegevens en de aankoop van sigaretten samen met een opwaardeerkaart. Onder bepaalde aannames kunnen deze deelonderzoeken met elkaar worden gecombineerd om een uitspraak te kunnen doen over de waarschijnlijkheid dat de verdachte de gebruiker was van de tipgevertelefoon. 'Dat betekent dat de bevindingen uit de diverse deelrapporten zeer veel waarschijnlijker zijn wanneer [verdachte] de gebruiker is van de tipgevertelefoon dan wanneer iemand anders dat is, aldus het NFI.'[20]

In aanvulling op de analyse van op zichzelf staande activiteiten is het ook mogelijk om eigenaarschap te bepalen door activiteiten gedurende langere tijdsintervallen te onderzoeken. Mensen zijn geneigd patronen te ontwikkelen in hun dagelijkse bezigheden. Interacties met digitale middelen registreren deze patronen.[21] Een persoon die elke werkdag om 08:00 uur in de ochtend instapt in de bus, laat niet alleen een registratie achter in het ov-systeem. De smartphone met stappenteller meet alle stappen van de voordeur tot de bushalte. In theorie zouden deze stappen elke werkdag ongeveer met elkaar overeen moeten komen. Een smartwatch geeft nog wat extra informatie, zoals de hartslagmeter. De gegevens van beide gegevensdragers kunnen elkaar complementeren.

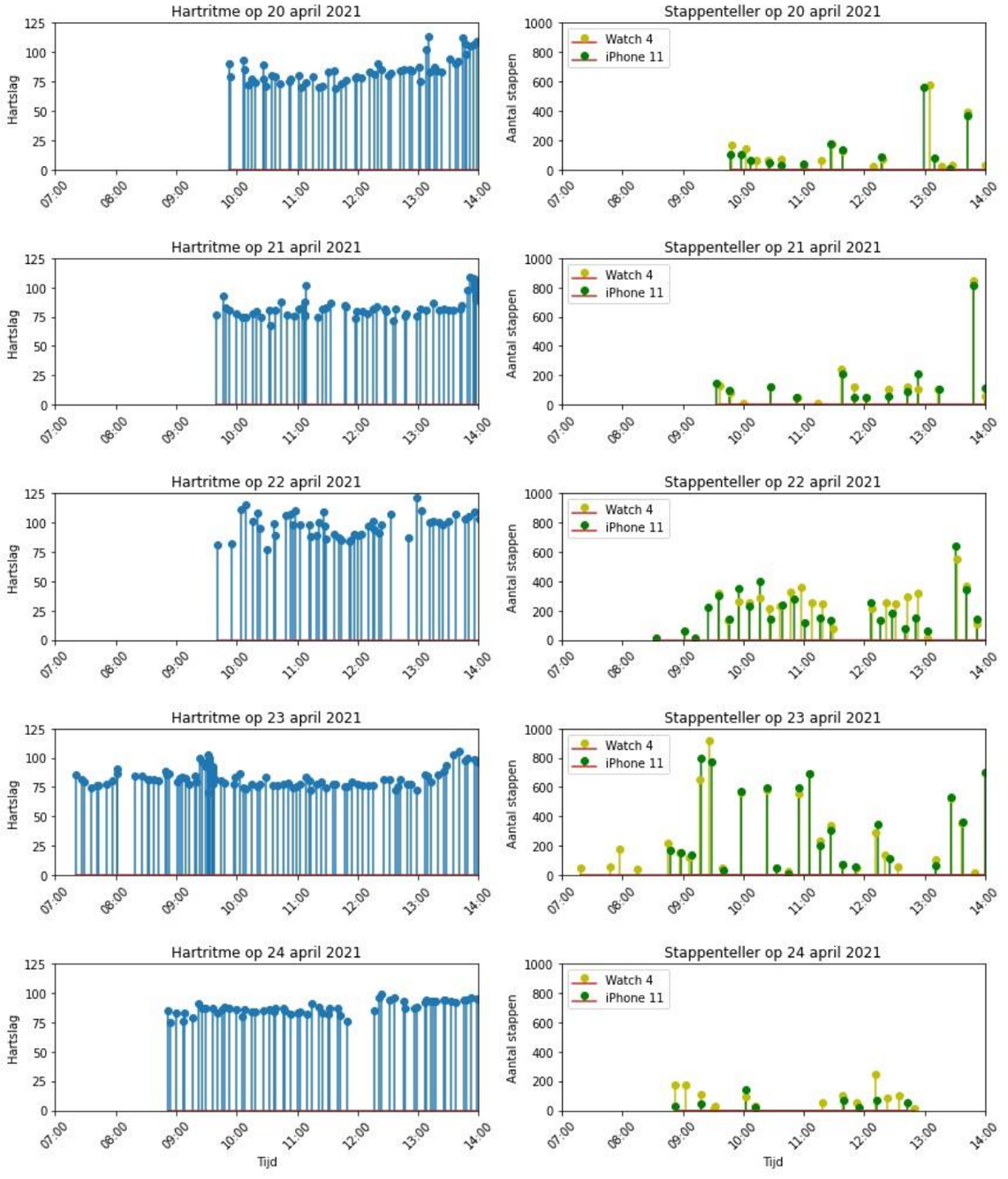
Figuur 1 op de volgende pagina illustreert de analyse van activiteiten gedurende vijf dagen in april 2021. Deze data zijn afkomstig van Matthew Sorell (Universiteit van Adelaide). Hij heeft toestemming gegeven om zijn persoonlijke smartwatch te gebruiken als testdata. Uit figuur 1 kunnen de volgende aannames worden herleid:

- De eerste drie dagen registreren de eerste hartslag vanaf 09:30 uur. Hieruit is op te maken dat de gebruiker zijn smartwatch niet in de nacht draagt. Mogelijk dat hij deze dan oplaadt.
- Op 22 april 2021 heeft de gebruiker eerst zijn iPhone gepakt en later heeft hij zijn smartwatch omgedaan. Op 23 april gebeurde precies het omgekeerde.
- Op 23 april 2021 is te zien dat de gebruiker rond 09:15 uur actief bezig is. Zo registreert de smartwatch meerdere hartmetingen, wat terug is te zien in het aantal stappen.
- 24 april 2021 heeft weinig hoge stappenregistraties. Mogelijk dat de gebruiker hier niet erg actief was. Dat kan kloppen, omdat dit een zaterdag betreft.

Om terug te komen op de gewoontes van de gebruiker: Sorell gaf aan dat hij meestal rond 10:00 uur begint met werken, wat overeenkomt met de eerste drie dagen van de metingen. Ook kon hij bevestigen dat hij zijn smartwatch in de avond oplaadt. Op 23 april bracht hij iemand weg, waardoor een vroege registratie te zien is van de smartwatch. Nu betreffen deze registraties slechts vijf dagen, maar de gehele dataset beslaat bijna vier jaar. Het is onmogelijk om elke dag te ontleden. Al zou het een maand voor en na het delict wel nuttig kunnen zijn om een dergelijke analyse uit te voeren. Het geeft namelijk niet alleen inzicht in de gebruiker, doorbrekingen van een patroon zeggen in sommige gevallen misschien wel meer.

Eigenaarschap vaststellen blijft in de praktijk nog lastig. Want hoewel biometrie potentieel gebruikt kan worden ter identificatie, registreert een iPhone niet genoeg gegevens om hierover een uitspraak te kunnen doen. Door verschillende digitale gegevensdragers te koppelen kunnen digitale sporen elkaar wel complementeren. Het meest treffende voorbeeld is de combinatie van een smartwatch en iPhone. Specifieke patronen of doorbrekingen hiervan zijn goede aanknopingspunten om verder op door te rechercheren. En hoe meer digitale sporen overeenkomen met verklaringen van een getuige of verdachte, des te aannemelijker het wordt dat deze de hoofdgebruiker is van de digitale gegevensdrager. Al is dit nooit 100% aannemelijk te maken.

19. ANPR is in het Nederlands beter bekend als kentekenplaatherkenning.
20. Rb. Oost-Brabant 19 december 2017, ECLI:NL:RBOBR:2017:6556.
21. Zie in de literatuurlijst Forensic Pattern Of Life Analysis.



Figuur 1. Aan de hand van de analyse van de hartslagmeter en stappenteller kunnen bepaalde patronen worden herleid. In de stappenteller is onderscheid gemaakt tussen de Apple Watch en de iPhone. Deze data komen uit de dataset van Matthew Sorell met een tijdsverschil van +09.30 UTC voor 20, 21 en 22 april en +08.00 UTC voor 23 en 24 april 2021. De tijdsverschillen zijn verwerkt naar lokale tijd van de gebruiker.

5. Met voorbedachte raad

Digitale sporen kunnen een indicatie geven over de – voor de vervolging belangrijke – vraag of handelingen al dan niet met voorbedachte raad zijn verricht. Zo oordeelde de rechtbank Limburg dat de door de verdachte voorafgaand aan het delict gebruikte zoektermen overtuigend genoeg waren om te spreken over moord in plaats van doodslag. Uit een analyse van de telefoon van de verdachte blijkt dat de zoektermen betroffen het overlijden voor en tijdens een scheiding. Het NFI achterhaalde deze zoektermen in de smartphone van de verdachte. De verdachte zou deze hebben opgezocht tussen mei en november 2015. Bij de zoekterm 'nekklem' bleek dat de verdachte een dag voor het delict had gezocht naar foto's hierover. Dit paste in het scenario waarbij het slachtoffer is omgebracht door middel van samendrukkend geweld op de nek/hals.[22] Mede op basis van deze zoektermen achtte de rechtbank de verdachte schuldig aan moord in plaats van doodslag. Uit deze

22. Rb. Limburg 28 maart 2018, ECLI:NL:RBLIM:2018:2940.

uitspraak blijkt dat digitale sporen kunnen bijdragen aan het bewijs van bijzondere delictsbestanddelen zoals opzet en voorbedachte raad.

Het combineren van verschillende digitale sporendragers geeft mogelijkheden om specifieke scenario's te verifiëren of falsificeren. Zo bleek in Griekenland een verklaring van een slachtoffer niet overeen te komen met data uit een smartwatch. Op 11 mei 2021 werd in Griekenland geschokt gereageerd op een brute moord op een jonge moeder. De echtgenoot van de vrouw vertelde aan de politie dat drie overvallers op zoek waren naar geld tijdens een inbraak bij hem thuis. De overvallers bonden hem en zijn vrouw op het bed, waarna ze allebei werden geblinddoekt. Dit gebeurde terwijl hun acht maanden oude dochtertje sliep. Zowel hun hondje als de moeder werd door verstikking om het leven gebracht. Het lukte de man uiteindelijk te ontsnappen, nadat de overvallers het huis hadden verlaten. De dochter bleef gedurende dit voorval ongedeerd. De politie loofde een beloning van € 300.000 uit voor informatie over deze overval.[23]

Het probleem was dat het verhaal van de man niet klopte met de digitale sporen die de rechercheurs vonden. Zo bleek dat het camerasysteem voorafgaand aan het delict werd uitgeschakeld. Ook gebruikte hij zijn telefoon op de momenten waarop hij verklaarde dat hij was vastgebonden.[24] Misschien de meest verontrustende data komen uit de smartwatch van de vrouw. Haar smartwatch registreerde nog haar hartslag rond de tijd waarvan haar man beweerde dat ze al om het leven was gebracht. Volgens de lijkschouwer was het tijdstip van overlijden tussen 04:05 en 04:11 uur. Uit de digitale data van de smartwatch concludeerde de lijkschouwer dat het slachtoffer op 11 mei tussen 01:41 en 03:51 uur sliep. Haar hartslag was consistent met een waarde tussen 48 en 58 hartslagen per minuut. Op 04:05 uur zou de hartslag met 50% toenemen, wat overeenkomt met een extreme vorm van fysieke of mentale stress. De laatste registratie was rond 04:11 uur. De lijkschouwer gaat ervan uit dat het slachtoffer daarna is overleden. Opvallend is dat de lijkschouwer vrij assertief handelde op de plaats delict. Ze zag namelijk dat het slachtoffer een smartwatch droeg. Ze stelde deze veilig, zodat de smartwatch in een forensisch laboratorium kon worden uitgelezen.[25] Als de lijkschouwer de smartwatch niet had gezien, dan waren mogelijk belangrijke sporen verloren gegaan. Deze resultaten in combinatie met het uitgeschakelde camerasysteem gaven genoeg aanwijzingen om de man aan te houden als verdachte.

Om te beantwoorden of sprake is van voorbedachte raad hoeven digitale experts niet alleen te vertrouwen op sporen voorafgaand aan het delict. Het opzoeken van specifieke zoektermen kan helpen bij beantwoording of sprake is van doodslag of moord. Echter, om specifiek het scenario te toetsen, heeft een digitaal expert meer mogelijkheden dan alleen een smartphone. Een smartwatch geeft op een macabere manier de laatste momenten van een slachtoffer weer. De laatste hartslag is letterlijk zichtbaar in de data.

6. Betrouwbaarheid

Digitale sporen zeggen in extreme gevallen meer dan traditionele forensische sporen. Een voorbeeld hiervan vinden we terug in België. Op 17 mei 2021 verliet Jürgen Conings zwaar bewapend de kazerne van Leopoldsburg. Hij zou het voorzien hebben op de viroloog Marc Van Ranst. Vanaf 19 mei 2021 zocht het federaal parket van België met man en macht naar Conings rond de plek waar hij zijn auto parkeerde. Op 20 juni kwam een einde aan deze zoektocht. Mountainbikers vonden het levenloze lichaam van Conings in Dilserbos. Het parket gaat ervan uit dat Conings zichzelf van het leven heeft beroofd. Om het tijdstip van overlijden te bepalen, voerde het Nationaal Instituut voor Criminalistiek en Criminologie (NICC) een entomologisch onderzoek uit. Hierbij wordt het tijdstip van overlijden bepaald aan de hand van insecten. Door de extreme hitte van die maand kon het NICC geen tijdstip van overlijden bepalen.[26]

Naast het entomologisch onderzoek is ook de gsm van Conings grondig geanalyseerd. Deze analyse bleek wel uitsluitsel te kunnen geven over het tijdstip van overlijden. De federaal procureur concludeerde namelijk: 'Wij weten dat die gsm 18 mei nog een stuk of 800 stappen heeft gezet en daarna is dat gestopt. Dus meer dan waarschijnlijk heeft hij zich van het leven beroofd de eerste dagen na zijn verdwijning'.[27] Het gegeven dat 800 stappen zijn gezet, geeft echter geen indicatie hoe betrouwbaar deze data zijn. Digitale sporen moeten in de context van de zaak geplaatst worden. Een net zo belangrijke vraag is: waar is de telefoon precies gevonden? Zoals in het artikel van Van Zandwijk en Boztas al vermeld werd, kan de plaatsing van de telefoon tijdens het wandelen invloed hebben op het aantal stappen dat de smartphone registreert.[28] Droeg hij zijn telefoon in zijn broekzak, jas of hand? Mogelijk dat de telefoon in een rugzak zat. Het antwoord op deze vraag kan weer invloed hebben op de beoordeling van mogelijke scenario's of hij zich op 18 mei van het leven beroofde of enkele dagen later.

Bij andere zaken zijn *pattern-of-life*-sporen aanvullend op eerder uitgevoerd onderzoek. In de nacht van 15 op 16 oktober 2016 fietste een negentienjarige vrouw, een student geneeskunde, door Freiburg im Breisgau, Duitsland. Rond 02:37 uur in de nacht vertrok ze van een faculteitsfeest. Ze is die nacht niet thuisgekomen. Een jogger vond haar levenloze lichaam in de ochtend langs de rivier Dreisam. Uit forensisch onderzoek bleek dat ze was verkracht en vermoord. De politie kreeg een verdachte in beeld dankzij een haar op de plaats delict en camerabeelden uit een tram. Naar aanleiding hiervan hield de politie een verdachte aan.[29] De verdachte beschikte in de nacht van het delict over een iPhone 4S. In de eerste instantie keek het onderzoeksteam naar de relatie tussen de iPhone en de nabijgelegen zendmastge-

23. Zie in de literatuurlijst Greece killing.
24. Zie in de literatuurlijst Griekse moordenaar valt door de mand.
25. Zie in de literatuurlijst Caroline Crouch.
26. Zie in de literatuurlijst Stappenteller met 800 stappen.
27. Zie in de literatuurlijst Stappenteller met 800 stappen.
28. Van Zandwijk & Boztas 2019.
29. Zie in de literatuurlijst Tote Studentin.

gevens. De locatie van de smartphone kwam qua tijd grotendeels overeen met de camerabeelden rond 02:10 uur. Om 02:46 uur was het laatste contact tussen de iPhone en een van de zendmasten. Pas om 04:02 uur had de iPhone weer contact met het telefoonnetwerk. Tussen 02:46 uur en 04:02 uur had het onderzoeksteam een gat in zijn scenario. Het team richtte zich daarom op de healthdb_secure-database. Het aantal geregistreerde stappen kwam overeen met eerder gevonden geolocaties. De iPhone registreerde ook nog iets opmerkelijks: twee keer traplopen. Deze registratie is op het eerste gezicht vreemd, want rond deze plek heeft de oever van de rivier geen trappen. Maar bij nader inzien paste het wel in het scenario dat de verdachte eerst het lichaam naar de oever sleepte en daarna weer terugklom. Om dit scenario te toetsen, heeft een rechercheur dezelfde bewegingen gereconstrueerd met een iPhone bij zich. Na het uitlezen bleek dat de smartphone de bewegingen als traplopen registreerde.[30]

Een smartphone beschikt over verschillende digitale sporen, die iets kunnen zeggen over activiteiten. Dat betekent niet per definitie dat deze altijd betrouwbaar zijn. Interpretatie van dit soort sporen blijft namelijk lastig. Digitale sporen kunnen worden gemanipuleerd.[31] Zelf een specifieke handeling reconstrueren en deze gegevens vergelijken met die van de verdachte helpt bij het verifiëren of falsificeren van bepaalde scenario's. Soms is dit echter niet mogelijk. In deze gevallen kan een expert de verklaringen van getuige of verdachte vergelijken met de beschikbare digitale sporen. Vergelijkbaar met toepassing om een eigenaar van een digitale gegevensdrager vast te stellen.

7. Conclusie

Het onderzoeksgebied *pattern-of-life forensics* in smartphones staat nog in de kinderschoenen. Dat komt mede doordat pas sinds 2018 zowel Apple als Google zijn begonnen met het toevoegen van zogenaamde *time trackers* op hun telefoons die altijd aanstaan. Dankzij deze *time trackers* heeft het onderzoek een flinke boost gekregen en zijn er meer mogelijkheden dan alleen het onderzoeken van bijvoorbeeld *health app*-gegevens. Onderzoekers krijgen steeds meer inzicht en merken ook dat andere apps ongemerkt allerlei gedragingen vastleggen die als digitaal spoor kunnen worden teruggevonden. Er is echter nog veel onbekend en de interpretatie van deze sporen is lastig. Bovendien veranderen apps voortdurend en daarmee kan de wijze van interpretatie per versie verschillen. Het is dus belangrijk om goed te documenteren welke versies aanwezig zijn en in sommige gevallen is het verstandig om met referentie-exemplaren te experimenteren om meer zekerheid te krijgen.

Het NFI heeft speciale software ontwikkeld waarmee automatisch vastgesteld kan worden waar de digitale sporen zitten, die gekoppeld kunnen worden aan de beweging van een telefoon. De software detecteert dat bestanden worden aangemaakt of gewijzigd tijdens een handeling, zoals het bewegen van de telefoon. Zo kunnen de onderzoekers dus snel bepalen in welke apps/logbestanden interessante informatie opgeslagen zit. In ENFSI-verband[32] wordt gewerkt aan AppAnalyze, waar onder andere het NFI aan bijdraagt. Het is de bedoeling dat in het AppAnalyze een database tot stand komt waarin wordt bijgehouden welke apps en welke versies welke sporen achterlaten. Met zo'n database wordt het in de toekomst eenvoudiger om digitale sporen te interpreteren.

Wanneer deskundigen meer inzicht krijgen in het verband tussen digitale sporen in smartphones en de handelingen van de gebruikers is het mogelijk om scenario's te verifiëren, falsificeren of wellicht zelfs te construeren. Op iedere smartphone bevinden zich verschillende *pattern-of-life*-sporen. Daarbij kan het ook nuttig zijn om door middel van experimenten inzicht te krijgen in statistieken omtrent veel uitgevoerde handelingen zodat ook in onzekere gevallen waarin het bewijs wordt betwist met *likelihood ratio's* het bewijs op een objectieve manier geëvalueerd kan worden. Tevens zou een deskundige rekening kunnen houden met zowel fysieke als digitale sporen, om een *likelihood ratio* te onderbouwen.

Literatuur

Brignoni
A. Brignoni, *Digital Forensics and Incident Response* <abrignoni.blogspot.com> (geraadpleegd 11 maart 2022).

Caroline Crouch
Greek City Times, *Caroline Crouch was fast asleep when Babis attacked* <greekcitytimes.com/2021/06/19/caroline-crouch-was-fast-asleep-when-babis-attacked/> (geraadpleegd 11 maart 2022).

Casey 2019a
E. Casey, 'The chequered past and risky future of digital forensics', *Australian Journal of Forensic Sciences* 2019, 51(6), p. 649-664.

Casey 2019b
E. Casey, 'Trust in digital evidence', *Digital Investigation* 2019, 31, 200898.

De Poot 2011
C. de Poot, *Wetenschap op de plaats delict* (lectorale rede Amsterdam), Amsterdam: Hogeschool van Amsterdam & Politieacademie 2011.

Die Version vom Handeln
Welt, *Die Version vom Handeln im Affekt ist mit dem heutigen Tag obsolet* <welt.de/vermischtes/article 172287105/Mordprozess-Hussein-K-Die-Version-vom-Handeln-im-Affekt-ist-mit-dem-heutigen-Tag-obsolet.html> (geraadpleegd 11 maart 2022).

Edwards
S. Edwards, mac4n6 <mac4n6.com/> (geraadpleegd 11 maart 2022).

30. Zie in de literatuurlijst Die Version vom Handeln.
31. Zuurveen & Stol 2020, p. 91.
32. European Network of Forensic Science Institutes (ENFSI) is een samenwerkingsverband, waarbij het delen van kennis en kunde centraal staat ter bevordering van forensisch onderzoek.

Flynn e.a. 2008
M. Flynn, R. Juergens & T. Cantrell, *Employing ISR SOF best practices*, National Defense University Washington DC Institute for National Strategic Studies 2008.

Forensic Pattern Of Life Analysis
Forensic Focus, *Forensic Pattern Of Life Analysis* <forensicfocus.com/articles/forensic-pattern-of-life-analysis/> (geraadpleegd 11 maart 2022).

Greece killing
British Broadcasting Corporation, *Greece killing: Pilot gives five-hour testimony in court* < bbc.com/news/world-europe-57570042> (geraadpleegd 11 maart 2022).

Griekse moordenaar valt door de mand
T. Kettenis, *Griekse moordenaar valt door de mand door sporthorloge* <ad.nl/buitenland/griekse-moordenaar-valt-door-de-mand-door-sporthorloge~acf4f065> (geraadpleegd 11 maart 2022).

Henseler & De Poot 2020
H. Henseler & C. de Poot, 'De betekenis van digitale sporen voor bewijs op activiteitniveau', *EeR* 2020, afl. 2, p. 50-59.

Jansen e.a. 2020
J. Jansen, T. van Valkengoed, S. Veenstra & W. Stol, *Kennis voor politiewerk in een digitale samenleving*, Cybersafety Research Group 2020.

Meconi 2021
T. Meconi, *Pattern-of-Life Forensics in Hansken. Maatwerk+ leveren met digitale sporen* <hsleiden.nl/binaries/content/assets/hsl/lectoraten/digital-forensics-en-e-discovery/publicaties/2021/pattern-of-life_forensics_in_hansken_v2.2.pdf> (geraadpleegd 11 maart 2022).

Stappenteller met 800 stappen
S. Sanen, *Stappenteller met 800 stappen op de gsm van Jürgen Conings doet vermoeden dat hij al kort na zijn verdwijning overleed* <vrt.be/vrtnws/nl/2021/08/24/stappenteller-op-gsm-juergen-conings-doet-vermoeden-dat-hij-al-k/> (geraadpleegd 11 maart 2022).

Tote Studentin
Welt, *Tote Studentin – Verdächtiger ist 17-jähriger Flüchtling* <welt.de/vermischtes/article159947230/Tote-Studentin-Verdaechtiger-ist-17-jaehriger-Fluechtling.html> (geraadpleegd 11 maart 2022).

Van Zandwijk & Boztas 2019
J. van Zandwijk & A. Boztas, 'The iPhone Health App from a forensic perspective: can steps and distances registered during walking and running be used as digital evidence?', *Forensic Science International: Digital Investigation* 2019, 28, p. S126-S133.

Van Zandwijk & Boztas 2021
J. van Zandwijk & A. Boztas, 'The phone reveals your motion: Digital traces of walking, driving and other movements on iPhones', *Forensic Science International: Digital Investigation* 2021, 37, 301170.

Zuurveen & Stol 2020
R. Zuurveen & W. Stol, *Benutten van Digitale Sporen*, Politiekunde 2020.