De betekenis van digitale sporen voor bewijs op activiteitsniveau

Henseler, Hans; de Poot, Christianne J.

published in
Expertise en Recht
2020

document version
Publisher's PDF, also known as Version of record

Hans Henseler en Christianne de Poot***

De betekenis van digitale sporen voor bewijs op activiteitniveau

Fysieke en digitale sporen worden vaak gebruikt in strafzaken om misdrijven te bewijzen. Fysieke sporen worden meestal geanalyseerd om daarmee de bron van het spoor te achterhalen, maar forensisch onderzoekers toetsen de laatste jaren vaker hypothesen op activiteitniveau aan de hand van fysieke sporen. Op dit moment wordt nog weinig aandacht besteed aan activiteitniveau in de context van digitale sporen. Historisch gezien is dit begrijpelijk omdat het tot voor kort nog lastig was om een persoon te koppelen aan een digitaal spoor. Maar nu smartphones, sociale media, slimme assistenten en horloges steeds persoonlijker worden, wordt in de bewijsvoering ook bij digitale sporen steeds vaker de vraag gesteld hoe het spoor is ontstaan. Het beantwoorden van die vraag kan helpen bij het vormen en toetsen van hypothesen en scenario's in het rechercheonderzoek.

Dit artikel begint met een introductie over het reconstrueren en bewijzen van activiteiten aan de hand van sporen. Vervolgens bespreken we een aantal Nederlandse strafzaken en analyseren we of en zo ja op welke wijze digitaal bewijs (mogelijk in samenhang met ander bewijs) is gebruikt om de activiteit van een verdachte te reconstrueren. Daarbij is zowel de digitale als de fysieke activiteit relevant nu onze fysieke ruimte en cyberspace in toenemende mate samensmelten. Dit artikel richt zich met name op de wijze waarop digitaal bewijs gebruikt kan worden bij het vormen en toetsen van hypothesen en scenario's op activiteitniveau, en op de betekenis hiervan voor de opsporingspraktijk.

1. Inleiding

Fysieke en digitale sporen worden vaak gebruikt in strafzaken om misdrijven te bewijzen. Fysieke sporen worden meestal geanalyseerd om daarmee de bron van het spoor te achterhalen. Zo kunnen relaties worden gelegd tussen een verdachte of een verdacht object en een gepleegd misdrijf. Het vaststellen van de bron van een spoor is echter niet altijd voldoende om een verdachte of verdacht object aan een misdrijf te relateren. Vaak moet daarvoor ook worden achterhaald door welke activiteit het spoor terecht is gekomen waar het werd aangetroffen. Daarvoor moeten activiteiten uit de sporen worden afgeleid en moeten hypothesen op activiteitniveau aan de hand van de sporen worden getoetst. Het analyseren van sporen op activiteitniveau is relatief nieuw en vindt plaats bij onderzoek naar DNA, vezels, glas, verf, schotresten en vingersporen.[1]

Smartphones en slimme apparaten bevatten uiteenlopende digitale sporen die een schat aan informatie bevatten voor forensisch onderzoek. In 2020 zullen naar verwachting zo'n 20 tot 30 miljard objecten met elkaar verbonden zijn in het Internet of Things (IoT).[2] Al deze apparaten laten digitale sporen na. Daarbij is zowel de digitale als de fysieke activiteit relevant nu onze fysieke ruimte en cyberspace in toenemende mate samensmelten.[3]

Zulke sporen zijn persoonlijker dan de traditionele digitale sporen uit e-mails en documenten omdat ze niet alleen ons bewuste gedrag maar in toenemende mate ook ons onbewuste gedrag laten zien. Deze ontwikkeling wordt mede veroorzaakt door de snelle opkomst van de kunstmatige intelligentie waardoor computersystemen in staat zijn om data uit allerlei sensoren in onze leefomgeving te interpreteren. Nu niet alleen de hoeveelheid maar ook de aard van de digitale informatie groeit, omvatten succesvolle zoekstrategieën veel meer dan alleen het lezen van e-mails, documenten en chats of het bekijken van foto's en video's.

Het bedenken en toetsen van scenario's is van oudsher een belangrijk onderdeel in het opsporingsonderzoek.[4] Voor een onderzoek is het soms belangrijker om te weten met wie is gecommuniceerd, waar iemand is geweest, wat die persoon heeft gedaan en wanneer, dan om te weten wat er is gecommuniceerd. Het kan interessant zijn om verbanden te leggen tussen verschillende apparaten en te onderzoeken welke activiteit er te vinden is rondom een specifieke gebeurtenis. Is er gezocht op bepaalde zoektermen, was de verdachte of het slachtoffer aan het wandelen, wat was de locatie van de smartphone of auto, wie waren er nog meer aanwezig op dat moment – het zijn vragen die kunnen helpen bij het reconstrueren wat er gebeurd kan zijn.

2. Digitaal bewijs op bronniveau vs. activiteitniveau

In een opsporingsonderzoek is bijna altijd de centrale vraag wie in verband gebracht kan worden met het misdrijf. Naast de wie-vraag zijn er nog een aantal standaard-

* Dr. ir. J. Henseler is Lector Digital Forensics & E-Discovery aan de Hogeschool Leiden en director bij Magnet Forensics.

** Prof. dr. C.J. de Poot is lector Forensisch Onderzoek aan de Hogeschool van Amsterdam en Politieacademie en hoogleraar Criminalistiek aan de Vrije Universiteit.

1. A. de Ronde e.a., 'The evaluation of fingermarks given activity level propositions', *Forensic Science International* (302) 2019, 109904. https://doi.org/10.1016/j.forsciint.2019.109904.
2. J.J. van Berkel e.a., *(Verkeerd) verbonden in het Internet of Things. Het Internet of Things, kansen, bedreigingen en maatregelen* (Cahiers 2017-8), Den Haag: WODC 2017. https://www.wodc.nl/binaries/2734_interactief_tcm28-267874.pdf.
3. J. Henseler, *De Revolutie van Digitaal Bewijs*, Hogeschool Leiden 2019. https://www.hsleiden.nl/binaries/content/assets/hsl/lectoraten/digital-forensics-en-e-discovery/publicaties/2017/lectorale-rede-hans-henseler-2017.pdf.
4. C.J. de Poot e.a., *Rechercheportret: over dilemma's in de opsporing*, Alphen aan den Rijn: Kluwer 2004.

vragen die helpen bij de opsporing van een strafbaar feit. Tezamen worden ze ook wel de zeven W-vragen genoemd:[5,6]

1. Wie kan in verband worden gebracht met het misdrijf?
2. Wat is er gebeurd?
3. Waar is het misdrijf gepleegd en waar kunnen mogelijk sporen gevonden worden?
4. Waarmee is het misdrijf gepleegd?
5. Op welke wijze is het misdrijf gepleegd?
6. Wanneer is het misdrijf gepleegd?
7. Waarom is het misdrijf gepleegd?

Antwoorden op deze vragen vormen de kernelementen van de gebeurtenis die moet worden gereconstrueerd. Digitaal bewijs kan uitstekend helpen bij het beantwoorden van deze vragen. De wie-vraag kan vaak beantwoord worden door te achterhalen welke gebruiker schuilgaat achter een e-mailadres, user account of telefoonnummer. Communicatie in sms, chat en e-mail geeft inzicht in wat er is gebeurd. Telecomgegevens, gps-locaties en wifinetwerken kunnen iets zeggen over de locatie waar een telefoon of een ander apparaat of zelfs een auto was. Foto's en video kunnen inzicht geven in de manier waarop en de middelen waarmee een misdrijf is gepleegd. Datum en tijd van een bestand of spoor kunnen iets zeggen over wanneer iets is aangemaakt, gewijzigd of gezien. Digitale data bieden dus een breed palet aan mogelijkheden waarmee naar antwoorden op de W-vragen kan worden gezocht, en waarmee scenario's over het misdrijf kunnen worden gevormd en getoetst.

Dit artikel gaat niet over digitaal bewijs op bronniveau maar over digitaal bewijs op activiteitniveau. Computers en smartphones houden gedetailleerd bij wanneer apps en gebruiker actief zijn geweest en welke bestanden zijn geraadpleegd. Afgezien van bewuste uitingen van een verdachte in e-mails en chatberichten kan bijvoorbeeld de zoekgeschiedenis uit een browser of uit specifieke apps inzicht geven in motief en/of voorbedachte rade terwijl de gebruiker zich niet bewust was dat zijn handelingen werden geregistreerd. In dit artikel gaan we in op de informatie over activiteiten die uit digitale sporen kan worden afgeleid.

In het onderzoek van De Ronde en collega's[7] wordt treffend het verschil uitgelegd tussen bronniveau en activiteitniveau in een situatie waarbij vingersporen op de plaats delict zijn aangetroffen:

Consider the following case example; a woman calls the police to report that there has been a burglary in her apartment. The police find four fingermarks on the railing of the balcony, which leads to the assumption that the perpetrator entered the apartment via the balcony. Through a database search, a match is found with a suspect, who is an acquaintance of the woman. The suspect claims that, instead of an unauthorized intrusion via the balcony, he visited the woman a week earlier and smoked a cigarette on the balcony while leaning on the railing. In cases like this, the question at stake changes from 'Who is the source of the fingermarks?' to 'What activity led to the deposition of the fingermarks?', which requires a different assessment of the findings.

In deze casus wordt de aanwezigheid van de vingerafdrukken van de verdachte op het balkon niet betwist, maar wordt betwist op welke wijze de vingerafdrukken daar terecht zijn gekomen. In de volgende paragraaf analyseren we het digitale bewijs in drie verschillende onderzoeken. Aan de hand van voorbeelden uit deze onderzoeken willen we illustreren waar digitaal bewijs kan helpen bij het toetsen van scenario's op activiteitniveau.

3. Digitaal bewijs in de praktijk

Voor onze analyse hebben we een drietal zaken geselecteerd uit rechtspraak.nl, namelijk:

1. Zaak 1: Moord op Koen Everink.
   Zie Rb. Midden-Nederland 23 januari 2018, ECLI:NL:RBMNE:2018:195
   en in hoger beroep https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHARL:2018:6296, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHARL:2019:2508
2. Zaak 2: Moord op de Bûterwei.
   Zie https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNNE:2019:2986
3. Zaak 3: Bezit van kinderporno.
   Zie https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2015:8015

Zaken 1 en 2 zijn uitgebreid in het nieuws geweest en daarin is ook melding gemaakt van het digitaal bewijs dat een rol speelde in het onderzoek. Zaak 3 is minder bekend maar is wel exemplarisch voor een groot aantal onderzoeken waarbij de verwerving en bezit van kinderpornografisch materiaal ten laste wordt gelegd.

Zaak 1: De moord op Koen Everink

Het slachtoffer is dood aangetroffen in de keuken van zijn woning. Hij is door messteken om het leven gebracht. De verdachte was de avond voorafgaand aan het delict aanwezig bij het slachtoffer en is vermoedelijk de laatste die het slachtoffer levend heeft gezien. De rechtbank vindt bewezen dat de verdachte het slachtoffer heeft omgebracht. De verdachte zegt onschuldig te zijn. Hij zou bij het verlaten van de woning ontvoerd zijn door meerdere mannen die bij hem in de auto stapten.

Het digitale bewijs dat in het vonnis van deze zaak wordt genoemd, heeft met name betrekking op de zoektermen die zijn gevonden op de iPad van de verdachte en de gezondheid-app op de iPhone van de verdachte.

5. H. Gross, *Handbuch für Untersuchungsrichter als System der Kriminalistik*, Berlijn: J. Schweitzer Verlag 1983.
6. C.J. de Poot, *Wetenschap op de plaats delict*, Lectorale rede, Hogeschool van Amsterdam & Politieacademie 2011.
7. A. de Ronde e.a., 'The evaluation of fingermarks given activity level propositions', *Forensic Science International* (302) 2019, 109904. https://doi.org/10.1016/j.forsciint.2019.109904.

Ten aanzien van de zoektermen op de iPad voert de verdediging aan dat bij het invoeren van zoektermen in een zoekmachine zoals Google, woorden of delen van woorden door de zoekmachine automatisch worden aangevuld. De verdediging stelt dat de zoekwoorden niet door de verdachte zijn ingevoerd, maar door de zoekmachine zelf zijn aangevuld.

De rechtbank gaat hier niet in mee en concludeert dat de verdachte voorafgaand aan dit misdrijf op zijn iPad heeft gezocht naar mogelijkheden om iemand uit te schakelen en naar mogelijkheden om iemand van het leven te beroven. Daarnaast heeft de verdachte voorafgaand aan het misdrijf gezocht op 'serienummer horloge iwc'. Het IWC-horloge dat bij het misdrijf uit de woning is weggenomen, is aangetroffen in het bezit van verdachte.

De gezondheid-app (stappenteller) komt ter sprake bij verlenging van het voorarrest van de verdachte op 23 september 2016. Later bij de bewijsmiddelen wordt de stappenteller niet meer genoemd. Uit andere open bronnen[8] valt op te maken dat de gegevens uit de stappenteller van de verdachte op zijn telefoon in strijd zijn met zijn alibi. De verdachte verklaarde dat hij in één ruk naar huis zou zijn gereden, maar volgens de stappenteller is hij tussentijds nog uitgestapt.

Zaak 2: Moord op de Bûterwei

In een weiland gelegen aan de Bûterwei (in de gemeente Dantumadeel) wordt het levenloze lichaam aangetroffen van het slachtoffer. Op korte afstand van zijn lichaam ligt zijn telefoon. Uit forensisch pathologisch onderzoek blijkt dat hij door geweld om het leven is gekomen. Naar aanleiding van het aantreffen van het lichaam wordt een grootschalig onderzoek opgestart, waarbij diverse scenario's worden onderzocht en waarbij ook het scenario partnerdoding wordt meegenomen. De echtgenote van het slachtoffer komt daarin als verdachte naar voren en wordt aangehouden.

Uit het gepubliceerde vonnis, aangevuld met informatie uit open bronnen,[9] blijkt dat het digitale bewijs een belangrijke rol heeft gespeeld in dit onderzoek.

- Het slachtoffer is door de verdachte met hun auto afgezet op een locatie vanaf waar hij met een boot naar een festivallocatie zou gaan. In het navigatiesysteem is het adres van de afzetlocatie teruggevonden.
- Uit onderzoek bleek dat de auto van de verdachte die avond ook nog is weggeweest. Na eerder te hebben verklaard dat ze niet was weggeweest die avond, verklaarde de verdachte dat ze misschien naar de glasbak was gereden.
- Kort na middernacht heeft verdachte een sms-bericht gestuurd naar het slachtoffer met de boodschap dat zij met hem in de buurt van het festival wil afspreken.
- Uit de mobiele telefoon van de verdachte blijkt dat zij iets later telefonisch contact heeft gehad met het slachtoffer. Verdachte heeft verklaard dat zij in dat gesprek met het slachtoffer heeft afgesproken dat zij hem zou komen ophalen.
- Ca. 10 minuten na het gesprek blijkt uit gebruikersactiviteiten en locatiegegevens in het Google-account van verdachte dat zij aanwezig was ter hoogte van de Bûterwei.
- Ca. 14 minuten later is de telefoon van verdachte uitgeschakeld door de gebruiker. Gedurende die tijd is de telefoon op dezelfde locatie gebleven. Gedurende die tijd heeft ze geen contact proberen te zoeken met de verdachte.
- Tussen het moment van het telefoongesprek en moment dat verdachte aankomt, blijkt uit onderzoek van de telefoon van het slachtoffer dat hij aan het lopen was.
- Ca. 6 minuten voordat de telefoon van verdachte wordt uitgeschakeld, verandert de hoek (verticaal of horizontaal) van het toestel van het slachtoffer. Drie minuten daarna beweegt het toestel niet meer en één minuut later verandert de hoek van het toestel weer aanzienlijk. Het is dan anderhalve minuut voordat het toestel van de verdachte wordt uitgeschakeld.
- De locatie van het toestel van verdachte verandert niet meer totdat het toestel de volgende ochtend op korte afstand van het lichaam van het slachtoffer wordt gevonden.
- Een getuige die het festivalterrein verliet, heeft een auto zien staan op tijdstip en plaats waar verdachte haar auto had geparkeerd. Getuige verklaart dat er niet één maar twee personen bij de auto stonden, vermoedelijk een man en een vrouw.
- Verdachte bevestigt dat zij daar is geweest op dat moment maar dat zij het slachtoffer niet heeft ontmoet zoals was afgesproken. Ze is daarna terug naar huis gereden zonder te stoppen met een snelheid van ca. 80 km per uur. Uit onderzoek van de beelden van beveiligingscamera's van drie verschillende bedrijven langs de route, blijkt dat de verdachte inderdaad te zien is op de beelden. Uit de tijdstippen blijkt echter dat ze over een afstand van 5,5 km in het totaal 18 minuten heeft gedaan en niet 8 minuten.
- Bij terugkomst 's nachts heeft de verdachte haar schoonouders gebeld en is ze samen met haar schoonvader (vader van het slachtoffer) op zoek gegaan. Verdachte beweert gedurende die zoektocht meerdere malen het slachtoffer gebeld te hebben maar dat blijkt niet uit het onderzoek naar haar telefoon. Daarop antwoordt ze dat ze gebeld heeft met het toestel van haar schoonvader, maar die ontkent dat.

8. Zie bijvoorbeeld het artikel in *Trouw* waarin verwezen wordt naar een vermoeden van de officier van justitie. https://www.trouw.nl/nieuws/om-eist-18-jaar-cel-voor-moord-op-everink~bc006e00.
9. Zie 'Hoe Google-data in een moordzaak leidden naar de echtgenote', *de Volkskrant* 8 augustus 2019. https://www.volkskrant.nl/nieuws-achtergrond/hoe-google-data-in-een-moordzaak-leidden-naar-de-echtgenote~b092755e.

Dankzij het digitale bewijs heeft de rechtbank de verdachte gewezen op een aantal vastgestelde feiten die niet sporen met de gegeven verklaringen. Bijvoorbeeld dat de accu van de telefoon niet leeg was. Ook blijkt uit locatiegegevens van de telefoon van verdachte en slachtoffer dat ze op enkele meters van elkaar waren verwijderd. Het is onwaarschijnlijk dat verdachte het slachtoffer niet heeft gezien. Ook is vastgesteld dat verdachte tijdens de terugreis 's nachts veel langzamer heeft gereden dan eerder verklaard en heeft ze de autorit de voorgaande avond verzwegen. Ten slotte bleek ook dat verdachte gelogen had over pogingen om het slachtoffer te bellen tijdens de nachtelijke zoektocht.

Uiteindelijk komt de rechtbank tot de conclusie dat het niet anders kan zijn dan dat de verdachte het slachtoffer die bewuste nacht wel heeft ontmoet en dat zij met hem het weiland is ingelopen waar hij met geweld om het leven is gebracht. Elk ander scenario waarbij de verdachte het slachtoffer niet heeft getroffen en iemand anders zonder dat verdachte daarvan afwist het slachtoffer om leven heeft gebracht, vindt de rechtbank onaannemelijk. Het dossier bevat na het zeer uitgebreide onderzoek, waarbij ook andere scenario's tegen het licht zijn gehouden, geen enkele concrete aanwijzing in die richting.

Zaak 3: Bezit van kinderporno

De verdenking komt er, kort en feitelijk weergegeven, op neer dat de verdachte gedurende een periode van vijf maanden kinderporno heeft verworven, in zijn bezit heeft gehad en zich daartoe met een geautomatiseerd werk/communicatiedienst de toegang heeft verschaft.

De verdediging stelt dat de verdachte vanuit zijn verslaving aan porno in aanraking is gekomen met de aangetroffen kinderpornografische afbeeldingen. De verdachte heeft grote torrent-bestanden gedownload met daarop ook afbeeldingen van extreme porno. Mogelijk zijn met deze torrent-bestanden ook kinderpornografische afbeeldingen meegekomen en heeft verdachte niet bewust gezocht naar kinderpornografisch materiaal.

In het proces-verbaal wordt beschreven dat een computer in beslag is genomen en dat daarop 635 afbeeldingen zijn aangetroffen die als kinderpornografisch kunnen worden aangemerkt. Van die foto's zijn er 106 toegankelijk en zijn de overige 529 gewist. De verbalisant heeft een selectie van 14 afbeeldingen samengesteld. De aanmaakdatum van deze afbeeldingen valt in de periode die in de tenlastelegging wordt genoemd.

Een andere verbalisant heeft de internetgeschiedenis op de computer onderzocht. Hij stelt vast dat er 176 zoekopdrachten zijn met een zoekterm waarvan de rechtbank waarneemt dat het gaat om afbeeldingen met een kinderpornografisch karakter. Hiermee wordt de verdachte geconfronteerd, die ter terechtzitting bevestigt dat hij op dat moment op zoek was naar kinderpornografisch materiaal.

De rechtbank overweegt dat het zoeken met dergelijke zoekopdrachten duidt op het doelgericht en daarmee opzettelijk binnenhalen van kinderpornografisch materiaal en verwerpt daarmee het verweer van de verdediging dat het kinderpornografisch materiaal per ongeluk zou zijn meegekomen bij het downloaden van grote torrent-bestanden. De afbeeldingen kunnen alleen op de computer terecht zijn gekomen indien verdachte bewust de bestanden heeft geopend.

4. Scenario's

In de bovenstaande zaken worden verschillende scenario's beschreven en getoetst aan de hand van het beschikbare bewijs. In onderstaande tabel worden de scenario's voor de verdediging en voor de aanklager kort samengevat en wordt aangegeven welk bewijs er is.

#	Scenario Verdediging	Scenario Aanklager	Bewijs
Zaak 1			
1	Zoekwoorden automatisch aangevuld door zoekmachine	Zoekwoorden door verdachte ingevuld	Zoekwoordsuggesties worden niet opgeslagen in het zoeklogbestand.
2	Verdachte is in zijn auto gebleven.	Verdachte is uit zijn auto geweest en heeft gelopen.	De stappenteller heeft rond dat tijdstip 210 stappen geregistreerd.
3	Verdachte beweert horloge te hebben gevonden dag na zijn ontvoering en toen pas te zijn gaan zoeken op internet.	Verdachte heeft voorafgaand aan het misdrijf gezocht op 'serienummer horloge iwc' en heeft het horloge bij het misdrijf uit de woning weggenomen.	Volgorde van zoektermen in de geschiedenis en een cookie waarmee een latere zoekopdracht gedateerd kan worden op een tijdstip op of voor 3 maart.
Zaak 2			
4	Verdachte zegt niet weggeweest te zijn op de avond voor de moord.	Rond 22:00 uur is verdachte met de auto naar een dorp verderop gereden, rijdt nog een stuk, stopt langs de kant van de weg, keert en rijdt weer naar huis.	Google-tijdlijn uit de Google Cloud die met het wachtwoord uit de iPhone van verdachte toegankelijk is gemaakt.
5	Telefoon van de verdachte stond uit omdat de batterij leeg was.	Verdachte heeft haar telefoon handmatig uitgezet.	Uit logbestanden van de telefoon blijkt dat de batterij van de telefoon niet leeg was.

#	Scenario Verdediging	Scenario Aanklager	Bewijs
6	Verdachte heeft slachtoffer naar de Bûterwei laten komen. Bij aankomst op de afgesproken ontmoetingsplaats heeft zij het slachtoffer niet gezien en is weer naar huis gegaan.	Verdachte heeft slachtoffer naar de Bûterwei laten komen. Zij heeft hem daar ontmoet en is met hem het weiland ingelopen, waar hij vervolgens op gewelddadige wijze om het leven is gebracht.	Aan de hand van Google Cloud-gegevens blijkt de telefoon van het slachtoffer om 00:27 nog te bewegen. Om 00:40 verandert de hoek van de telefoon aanzienlijk en om 00:43 is er geen beweging. De telefoon ligt dan op de locatie waar het slachtoffer die ochtend is gevonden. Uit locatiegegevens van beide telefoons blijkt dat beide omstreeks die tijd binnen een afstand van 15-20 meter van elkaar zijn geweest.
7	Verdachte heeft slachtoffer gebeld tijdens de zoektocht 's nachts.	Verdachte heeft slachtoffer niet gebeld tijdens de zoektocht 's nachts.	Belgeschiedenis van telefoon verdachte laat geen belpogingen zien.
8	Verdachte is met 80 km/uur naar huis gereden zonder te stoppen.	Verdachte is niet rechtstreeks naar huis gereden maar is onderweg gestopt.	Uit beveiligingscamera's langs de route blijkt dat de gemiddelde snelheid 18 km/uur bedroeg.
Zaak 3			
9	Bestanden zijn per ongeluk gedownload als onderdeel van een torrent-bestand (container).	De bestanden zijn door de verdachte bewust gedownload en bekeken.	Bestanden staan in map van bestanden die zijn geopend in een internetbrowser en dus zijn bekeken.
10	Verdachte heeft niet bewust gezocht naar kinderpornografisch materiaal.	Verdachte heeft bewust gezocht naar kinderpornografisch materiaal.	Verdachte heeft 176 keer gezocht op een zoekterm die duidt op het doelgericht en daarmee opzettelijk binnenhalen van kinderpornografisch materiaal.

Kijken we naar de betekenis van dit digitale bewijs voor de reconstructie van activiteiten, dan zien we in zaak 1 dat de verdachte niet betwist dat hij op internet heeft gezocht naar het merk horloge, maar dat hij zegt dat hij dit pas de dag na de moord heeft gedaan. Dankzij de volgorde van de zoektermen in de zoekgeschiedenis in combinatie met de mogelijkheid om een andere zoekopdracht te koppelen aan een cookie met tijdstempel, kon de activiteit die uit het digitale materiaal kon worden afgeleid geplaatst worden in de tijd, en kon aannemelijk worden gemaakt dat verdachte al voor de moord gezocht had naar het merk horloge.

Zo ook met de verdachte in zaak 2 die beweert dat de batterij van haar telefoon leeg was. Het feit dat de telefoon uitstond op het bewuste moment, wordt niet betwist. Wel wordt betwist dat de telefoon door de gebruiker is uitgezet. Volgens de verdachte was de batterij leeg maar digitale sporen laten zien dat dat niet zo was. In deze zaak vormt de combinatie van locatiegegevens uit de Google Cloud van het slachtoffer, de oriëntatie van zijn telefoon en de registratie van gebeurtenissen door deze telefoon sterk bewijs voor het scenario van de aanklager. Deze sporen vormen zeer bruikbare aanwijzingen van wat er op welk moment met het slachtoffer is gebeurd, en aan de hand van deze sporen kunnen verklaringen hierover worden getoetst.

In zaak 3 zijn er belastende foto's gevonden op de computer van de verdachte. De aanwezigheid van de foto's wordt niet betwist maar de vraag is of die foto's daar per ongeluk of opzettelijk terecht zijn gekomen. De verdachte verdedigt zich door te zeggen dat de foto's daar per ongeluk zijn gekomen. De gevonden zoekterm en het feit dat de foto's niet in een container zitten maar zijn uitgepakt, vormen bewijs voor bewuste activiteiten, waarmee de rechtbank wordt overtuigd van opzet.

5. Ontwikkelingen in digitaal forensisch onderzoek

Door de snelle ontwikkelingen op het gebied van smartphones en het IoT, ontwikkelt het digitaal forensisch onderzoek zich in een hoog tempo. Zo'n tien jaar geleden lag de nadruk in het onderzoek nog vooral op de analyse van bestanden (*file forensics*). Tegenwoordig zijn *software tools* vooral gericht op artifacts omdat de metadata van bestanden (bestandsnaam, datum enz.) weinig zeggen over de gegevens die in het bestand zijn opgeslagen. Zo worden in een Windows-computer bijvoorbeeld vele tienduizenden eigenschappen en gebeurtenissen geregistreerd in een registry-bestand of een gebeurtenissenbestand (*eventlog*).

In 2018 is zowel Apple als Google begonnen met het toevoegen van zogenaamde *time trackers* op hun telefoons. Google heeft deze functionaliteit de naam *Digital Wellbeing* gegeven en Apple noemt deze functionaliteit *Screen Time*. *Digital Wellbeing* is beschikbaar vanaf Androidversie 9 Pie; Screen Time vanaf Apple iOS 12. Oudere smartphones en smartphones van bepaalde merken beschikken mogelijk nog niet over deze functionaliteit, ook al zijn ze bijgewerkt met een nieuwere versie van het besturingssysteem.

Zowel *Digital Wellbeing* als *Screen Time* geeft inzicht in de hoeveelheid tijd die door de smartphone wordt gebruikt, het aantal unlocks, notificaties en meer. Die informatie wordt bijgehouden door het besturingssysteem aan de hand van een administratie waarin in detail het gebruik van de telefoon en apps geregistreerd wordt. Digitaal forensisch onderzoekers hebben uitgeplozen in welke bestanden en in welk formaat deze eigenschappen worden opgeslagen. Zo houdt Apple in iOS de administra-

tie bij in de KnowledgeC-tabellen waarover wordt gerapporteerd door onafhankelijk onderzoekers[10] maar ook door ontwikkelaars van commerciële tools.[11]

Deze uitbreidingen van de twee populairste smartphonebesturingssystemen zijn illustratief voor de rijkdom aan digitaal forensische sporen die door andere smartphoneapps en IoT-apparaten worden bijgehouden. De stappenteller in zaak 1 is daar een goed voorbeeld van. De kunst is om de sporen uit zulke apps zodanig te combineren dat er bewijs geleverd kan worden dat waarschijnlijker is in het ene scenario dan in het andere. De rechter bepaalt welk scenario uiteindelijk het waarschijnlijkst is. Hieronder worden vier voorbeelden uitgewerkt die illustreren hoe verschillende sporen gezamenlijk een activiteit in kaart kunnen brengen:

Voorbeeld 1: Foto gemaakt met de telefoon of niet?
In dit voorbeeld is het van belang om te weten of de verdachte op een bepaald tijdstip op een bepaalde plaats is geweest. Van de verdachte is een *smartphone* in beslag genomen die is onderzocht. Ook zijn er telecomgegevens (*call detail records*) van het abonnement opgevraagd maar daaruit blijkt dat er op het bewuste tijdstip geen telefoonverkeer is geweest. Op de smartphone wordt wel een foto aangetroffen met de locatiegegevens van de desbetreffende plaats. De verdediging stelt dat de verdachte deze foto via e-mail heeft ontvangen en dat deze zodoende op zijn telefoon terecht is gekomen.

Uit nader onderzoek van de smartphone blijkt dat vlak voor het tijdstip waarop de foto is genomen, de telefoon is ontgrendeld, waarna de camera-applicatie op de telefoon is gestart. Aansluitend wordt het bestand aangemaakt met daarin de foto die eerder is aangetroffen en waarin de locatie van de plaats waar de telefoon zich op dat moment bevindt, wordt opgeslagen. Hiermee wordt het bewijs geleverd dat de bewuste foto op dat moment met de camera van de smartphone is gemaakt.

Wanneer gekeken wordt naar de details van het fotobestand (zie Figuur 1), dan blijkt dat er een locatie is opgeslagen in de zogenaamde Exif-metadata van het bestand. Gelet op de activiteiten is het waarschijnlijk dat dit de locatie is waarop de telefoon zich op dat moment bevond. De gegevens uit de tweede en laatste regel in Figuur 1 zijn niet afkomstig van de telefoon maar uit de Google Cloud waarvan ook een kopie is gemaakt.

Bovenstaand voorbeeld is afgeleid van een ouder type *smartphone* met het Android besturingssysteem. Nieuwere iPhones leggen activiteiten vast in de KnowledgeC-tabellen waarin nog meer details zijn te vinden over de acties die met de telefoon zijn uitgevoerd. In Figuur 2 op de volgende pagina is te zien dat eerst 'Screen off' wordt beëindigd, dan dat de telefoon ontgrendeld wordt, en dat de telefoon ongeveer 5 seconden rechtop (verticaal) is gehouden. In verticale toestand is de camera-applicatie gestart. Nadat de telefoon weer plat (sideways) ligt, is te zien dat een fotobestand (IMG_0014.JPG) wordt gemaakt gevolgd door een filmpje (IMG_0014.MOV), omdat de *Live Photos* functie van de iPhone aanstaat. Ten slotte wordt de camera-applicatie afgesloten.

Voorbeeld 2: Waar is naar gezocht en wanneer?
Uit de hierboven genoemde strafzaken blijkt dat de zoekgeschiedenis die wordt aangetroffen op een computer of smartphone belangrijk bewijs kan vormen. Voor het toetsen van scenario's kan het belangrijk zijn om te achterhalen of een zoekterm door de gebruiker is ingevoerd en zijn de datum en het tijdstip van het zoeken van belang.

Het is gebruikelijk om zoekvragen bij gangbare zoekmachines (bijv. Google, Bing, Yahoo en Facebook) te detecteren in de browsergeschiedenis en die apart aan de gebruiker te tonen. In de browsergeschiedenis zijn datum en tijd bekend. Bijkomstig probleem echter is dat er inmiddels een grote variëteit aan webbrowsers bestaat. Om de zoekgeschiedenis van een gebruiker inzichtelijk te maken, zal dus eerst de internethistorie van alle beschikbare browsers op het apparaat veilig moeten worden gesteld. De bekendste browsers zijn Chrome, Firefox, Edge, Internet Explorer en Safari, maar dan zijn er nog tientallen andere bekende en minder bekende browsers. Bovendien kunnen de technische details van één type browser verschillen afhankelijk van het platform (Windows, MacOS, iOS, Android).

10/6/2016 9:21:15 AM	First Active Date/Time	Program execution	Operating...	Application Activity -...	com.google.android.GoogleCamera
10/6/2016 9:21:15 AM	Date/Time	Device interaction	Cloud	Cloud Google Activity	Used
10/6/2016 9:21:21 AM	Created Date/Time	File knowledge	Media	Pictures	IMG_20161006_092119.jpg
10/6/2016 9:21:21 AM	Last Accessed Date/Time	File/folder opening	Media	Pictures	IMG_20161006_092119.jpg
10/6/2016 9:21:21 AM	Last Modified Date/Time	File/folder opening	Media	Pictures	IMG_20161006_092119.jpg
10/6/2016 9:21:21 AM	Photo Timestamp Date/Time	File/folder opening	Cloud	Cloud Google Photos...	IMG_20161006_092119.jpg
10/6/2016 9:21:21 AM	Created	File knowledge	File system	Folder	IMG_20161006_092121
10/6/2016 9:21:21 AM	Accessed	File/folder opening	File system	Folder	IMG_20161006_092121
10/6/2016 9:21:21 AM	Modified	File/folder opening	File system	Folder	IMG_20161006_092121
10/6/2016 9:21:21 AM	Created	File knowledge	File system	File	IMG_20161006_092119.jpg

Software	**bullhead-user 7.0 NRD90S 3142244 release-keys**
Make	**LGE**
Model	**Nexus 5X**
GPS Latitude	**38°25'20.86"**
GPS Latitude Reference	**North**
GPS Longitude	**82°25'52.21"**
GPS Longitude Reference	**West**
Altitude (meters)	**154.0**
MD5 Hash	**22d83f038a1127178d806add2f2e38d3**

Figuur 1: Reeks van gebeurtenissen. Links: camera-app wordt uitgevoerd (bovenste regel), fotobestand gecreëerd wordt in Google Cloud opgeslagen. Rechts: metadata van het fotobestand met o.a. gps-locatie en hoogte.

10. Bijvoorbeeld in S. Edwards, 'Knowledge is Power! Using the macOS/iOS knowledgeC.db Database to Determine Precise User and Application Usage', 6 augustus 2018, via: https://www.mac4n6.com/blog/2018/8/5/knowledge-is-power-using-the-knowledgecdb-database-on-macos-and-ios-to-determine-precise-user-and-application-usage.
11. Zie bijvoorbeeld 'Getting Evidence from iOS Screen Time Artifacts', *Magnet Forensics Blog*, 19 december 2018, via: https://www.magnetforensics.com/blog/getting-evidence-from-ios-screen-time-artifacts en M. Goldberg, 'How a Suspect's Pattern-of-life Analysis is Enhanced with KnowledgeC Data', *Cellebrite Blog,* 13 juni 2019, via: https://www.cellebrite.com/en/blog/how-a-suspects-pattern-of-life-analysis-is-enhanced-with-knowledgec-data.

11/1/2019 9:41:44 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Screen Backlight...	State	Screen off
11/1/2019 9:41:47 AM	Recorded Date/Time	Device interaction	Operating Syst...	KnowledgeC Screen Backlight...	State	Screen off
11/1/2019 9:41:48 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Lock States	State	Locked
11/1/2019 9:41:49 AM	Recorded Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Lock States	State	Locked
11/1/2019 9:41:52 AM	Start Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Vertical
11/1/2019 9:41:53 AM	Start Date/Time	Device interaction	Operating Syst...	KnowledgeC Application Focus	Application...	com.apple.camera
11/1/2019 9:41:56 AM	Start Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Sideways
11/1/2019 9:41:56 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Vertical
11/1/2019 9:41:59 AM	Recorded Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Vertical
11/1/2019 9:42:03 AM	Date/Time		Unknown	Unknown	Date/Time -...	2019-11-01 08:42:03
11/1/2019 9:42:04 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Device Orientatio...	State	Sideways
11/1/2019 9:42:05 AM	Date/Time		Unknown	Unknown	Sender	FA4F3997-EEB7-4A2A-
11/1/2019 9:42:05 AM	Last Modified Date/Ti...	File/folder openi...	Media	Pictures	File Name	IMG_0014.JPG
11/1/2019 9:42:05 AM	Last Modified Date/Ti...	File/folder openi...	Media	Live Photos	File Name	IMG_0014.JPG
11/1/2019 9:42:05 AM	Last Modified Date/Ti...	File/folder openi...	Media	Videos	File Name	IMG_0014.MOV
11/1/2019 9:42:05 AM	Modified	File/folder openi...	File system	File		IMG_0014.JPG
11/1/2019 9:42:05 AM	Modified	File/folder openi...	File system	File		IMG_0014.MOV
11/1/2019 9:42:06 AM	End Date/Time	Device interaction	Operating Syst...	KnowledgeC Application Focus	Application...	com.apple.camera

Figuur 2: Tijdlijn met activiteiten afkomstig uit o.a. de KnowledgeC-tabellen waaruit op grond van technische feiten blijkt dat een foto is gemaakt met de telefoon.

In Figuur 3 wordt een deel van de Google-zoekgeschiedenis getoond uit de Chrome-internetgeschiedenis op een Windows 10-computer. Zowel de zoekterm ('Search Term') als de oorspronkelijke zoekterm ('Original Search Query') wordt getoond met de datum en tijd van het moment waarop gezocht werd. Dat wat wordt ingetypt door de gebruiker wordt in het besturingssysteem vastgelegd als de oorspronkelijke zoekterm ('Original Search Query'). Google zal dan tijdens het typen in de browser suggesties doen van zoektermen. Als de gebruiker zo'n suggestie kiest, zal de gezochte zoekterm afwijken van de oorspronkelijke zoekterm.

Google houdt van gebruikers (die daar toestemming voor hebben gegeven) activiteit bij in de Google Cloud. Bijvoorbeeld of de gebruiker op een advertentie heeft geklikt of deze juist heeft genegeerd, op wat voor woorden is gezocht, welke apps zijn gebruikt, welke video's op YouTube zijn bekeken, enz. Weliswaar is deze informatie in veel gevallen ook op de telefoon terug te vinden maar de geschiedenis in de cloud gaat meestal verder terug en bovendien geeft Google nu expliciet aan dat het gaat om activiteit van één bepaalde, op grond van zijn gebruikersaccount te identificeren, gebruiker van de telefoon.

Ook het zoeken in Google Maps wordt vastgelegd en het opvragen van een routebeschrijving wordt expliciet als activiteit opgeslagen. In Figuur 4 op de volgende pagina is een voorbeeld gegeven waarin de gebruiker op zoek is naar een routebeschrijving ('Directions to'). De tijd wordt weergegeven en ook de URL die is bewaard. In die URL staan het vertrekpunt (hier Schiphol) en een bestemming aangegeven (hier met lengte- en breedtegraad).

Search Term	Date/Time	Original Search Query	Sea
connect smartwatch to iphone	10/30/2019 1:17:47 AM	connect smart watch to	
guardian uk	10/30/2019 12:08:02 PM	guard	
guardian uk	10/30/2019 12:08:07 PM	guard	
bbc news	10/30/2019 12:08:10 PM	bbc	
guardian uk	10/30/2019 12:08:11 PM	guard	
bbc news	10/30/2019 12:08:13 PM	bbc	
youtube	10/30/2019 12:09:31 PM	yo	
youtube	10/30/2019 12:09:33 PM	yo	
stock exchange cnn	10/30/2019 12:10:47 PM	stock	
earpods amazon	10/30/2019 15:31:11 PM	earpods am	
earpods amazon	10/30/2019 15:31:13 PM	earpods am	

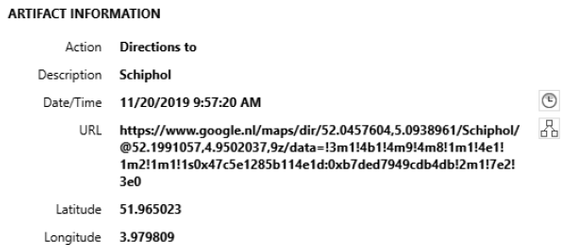
DETAILS

ARTIFACT INFORMATION

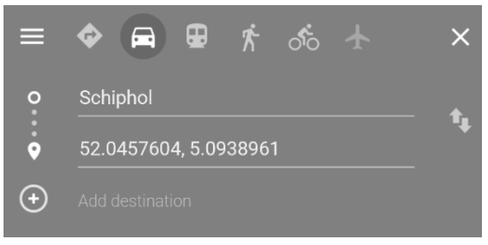
Search Term	**guardian uk**
URL	**https://www.google.com/search?q=guardian+uk&oq=guard&aqs=chrome.0.69i59j69i57j69i59j69i60l3.2458j0j7&sourceid=chrome&ie=UTF-8**
Date/Time	**10/30/2019 12:08:02 PM**
Original Search Query	**guard**
Web Page Title	**guardian uk - Google Search**
Original artifact	Chrome Web Visits

Figuur 3: Voorbeeld van Google searches die zijn gevonden op een Windows 10 computer. Links is de zoekterm te zien met datum/tijd en de oorspronkelijke zoekvraag. Rechts wordt het record in detail getoond voor de zoekterm in de op één na bovenste regel links 'guardian uk'.

(a)



(b)



Figuur 4: De gebruiker heeft via Google Maps een route opgevraagd vanaf Schiphol: (a) Artifact uit de Google Cloud activity van een Android smartphone; (b) Weergave in Google maps indien de URL naar Google wordt verstuurd in een webbrowser.

Voorbeeld 3: Downloadbestanden

In dit derde voorbeeld staat een scenario centraal waarin een fotobestand is aangetroffen op een computer, en is het de vraag hoe dat bestand daarop terecht is gekomen. Eén scenario is dat de gebruiker de bestanden heeft gedownload. Een ander scenario is dat de gebruiker het bestand vanaf een usb-stick heeft gekopieerd. Figuur 5 illustreert een tijdlijn van sporen die erop duiden dat de gebruiker een e-mail heeft geopend, en van daaruit naar de website Reddit is gegaan waar een fotobestand is gedownload.

Internetbrowsers zoals Chrome, Safari, Firefox en Edge laten vrij gedetailleerde sporen achter over de wijze waarop websites zijn bezocht en bestanden zijn gedownload. Neem als voorbeeld Chrome en in het bijzonder *Chrome Web History*, *Chrome Web Visits* en *Chrome Downloads*. De eerste houdt bij welke URL is bezocht, het tijdstip waarop die het laatst is bezocht en het aantal keren dat het adres is bezocht. *Chrome Web Visits* houdt exact de datum en het tijdstip bij waarop een URL is bezocht en of het adres door de gebruiker is ingetypt, doorgeklikt enz. Ten slotte houdt Chrome Downloads bij welke bestanden zijn gedownload met Chrome, van welk adres het bestand afkomstig is, waar het is opgeslagen, op welk moment en of het geopend is na het downloaden (zie Figuur 6).

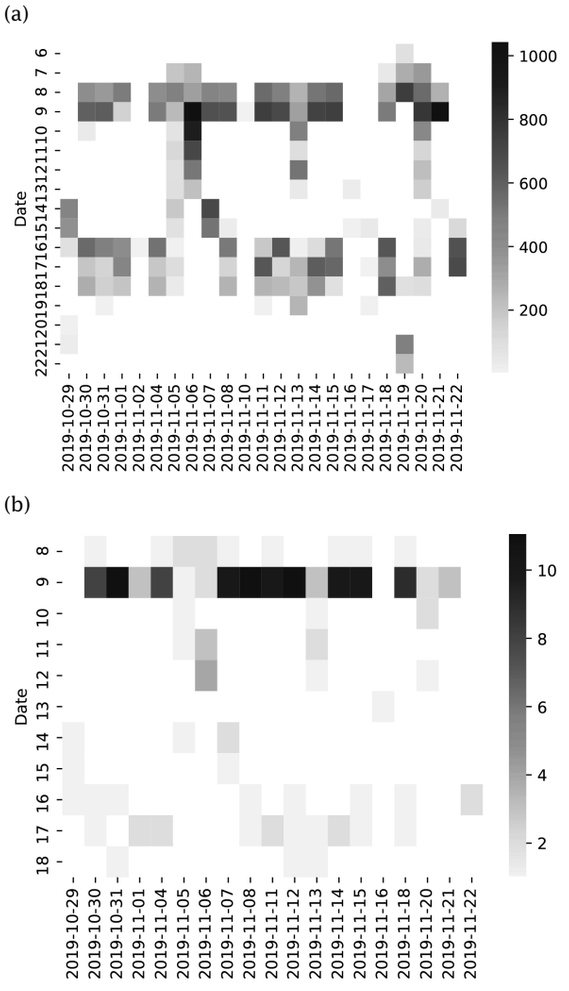
Figuur 6: Chrome web visit-spoor van een download op een Windows 10 computer. De data laten zien dat het bestand 'ideas.zip' in zijn geheel is gedownload en vervolgens door de gebruiker is geopend.

Voorbeeld 4: Was de telefoon op een bepaald moment in gebruik?

De Health-app op een iPhone houdt gegevens bij die registreren hoeveel de gebruiker beweegt. De app telt automatisch Steps, Distance en Floors en op welk moment er beweging is (Figuur 7). Op vergelijkbare wijze worden ook veranderingen in de oriëntatiestatus van een telefoon bijgehouden (staand of liggend), hetgeen ook iets zegt over beweging. We kunnen dus niet alleen achterhalen of de telefoon op een bepaald moment in gebruik was maar ook aangeven of de telefoon is verplaatst.

8/29/2016 19:15:38 PM	Date Visited Date/Time	Browser usage	Web Related	Chrome Web Visits	URL	https://mail.google.com/mail/#inbox
8/29/2016 19:15:41 PM	Date Visited Date/Time	Browser usage	Web Related	Chrome Web Visits	URL	https://out.reddit.com/t3_4yxb3z?url=https%3
8/29/2016 19:15:41 PM	Date/Time	Browser usage	Refined Results	Social Media URLs	Site Name	Reddit
8/29/2016 19:15:41 PM	Date Visited Date/Time	Browser usage	Web Related	Chrome Web Visits	URL	https://drscdn.500px.org/photo/168898645/q:
8/29/2016 19:15:41 PM	Last Visited Date/Time	Browser usage	Web Related	Chrome Web History	URL	https://out.reddit.com/t3_4yxb3z?url=https%3
8/29/2016 19:15:41 PM	Last Visited Date/Time	Browser usage	Web Related	Chrome Web History	URL	https://drscdn.500px.org/photo/168898645/q:
8/29/2016 19:15:41 PM	Date/Time	Browser usage	Refined Results	Social Media URLs	Site Name	Reddit
8/29/2016 19:15:47 PM	Last Accessed Date/Time	File/folder opening	Media	Pictures	File Name	stock-photo-168898645.jpg
8/29/2016 19:15:47 PM	Start Time Date/Time	File download	Web Related	Chrome Downloads	Download Source	https://drscdn.500px.org/photo/168898645/q:

Figuur 5: Tijdlijn met activiteiten die laten zien dat een fotobestand is gedownload door een gebruiker, na het lezen van een e-mail in de inbox van Gmail.



Figuur 7: Overzicht van activiteit op basis van de Apple Health app. (a) afstand (distance) per dag/uur, (b) het aantal verdiepingen (floors) per dag/uur.

Of de telefoon in gebruik is, kan op verschillende manier aangetoond worden. Allereest wordt bijgehouden of de telefoon *locked* of *unlocked* is (*KnowledgeC Device Lock States*). Daarnaast wordt ook bijgehouden welke app in focus is (*KnowledgeC Application Focus* en *Application Activities*) en tot op zekere hoogte probeert het systeem zelfs bij te houden wat de intenties zijn van een applicatie (*KnowledgeC Application Intents*).

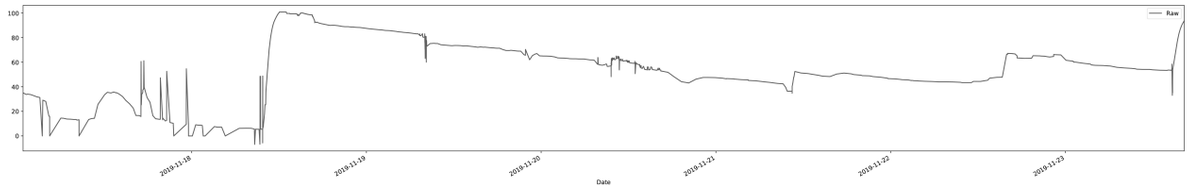
Als laatste voorbeeld wordt in Figuur 8 geïllustreerd dat het ook mogelijk is om het spanningsniveau van de batterij gedurende de afgelopen periode (van een aantal dagen) te visualiseren. De figuur begint wat grillig maar na verloop van tijd is te zien dat de batterij van de telefoon in deze periode nooit leeg is geweest en vanaf 19 november één keer per dag een klein beetje wordt opgeladen.

Ten slotte is het ook mogelijk om naar locatiegeschiedenis te kijken die op een smartphone of computer aanwezig is in de vorm van gps-locaties en wifinetwerken die aan een locatie te koppelen zijn. Die informatie kan niet gebruikt worden om een kleine beweging (bijvoorbeeld het oppakken van de telefoon of het zetten van een paar stappen) vast te stellen maar wel om de locatie van een telefoon aan de hand van gps-coördinaten vast te stellen en eventueel om een verplaatsing vast te stellen als tijdstippen geregistreerd zijn.

6. De betekenis van digitale sporen voor bewijs op activiteitniveau

De zaken en de voorbeelden die we hierboven beschreven, laten zien dat digitale sporendragers en digitale sporen een schat aan informatie bevatten waarmee scenario's over misdrijven kunnen worden gevormd, worden aangepast en worden getoetst.

Bewijsmiddelen verschillen van elkaar als het gaat om de mate waarin ze activiteiten kunnen bewijzen. Uit verklaringen van slachtoffers en getuigen kunnen soms complete scenario's over wat er is gebeurd worden gereconstrueerd. Ooggetuigen kunnen soms verslag doen over wat er op welk moment in welke volgorde is gebeurd. Ook camerabeelden kunnen soms een complete weergave bieden van de activiteiten die zijn verricht. Fysiek sporenmateriaal verschilt van dit soort bewijs, enerzijds omdat gebeurtenissen slechts een beperkt aantal fysieke gevolgen hebben, en anderzijds omdat die fysieke gevolgen (de sporen op de plaats delict of op het lichaam van een slachtoffer) in de meeste gevallen door verschillende gebeurtenissen veroorzaakt zouden kunnen zijn. Fysiek sporenmateriaal wordt vooral gebruikt om hypothesen over specifieke elementen van de gebeurtenis te vormen en om scenario's te toetsen die uit overig opsporingsmateriaal – bijvoorbeeld uit verklaringen van slachtoffers, verdachten of getuigen – zijn voortgevloeid.[12] Met preciezere sporenanalyses zijn we tegenwoordig steeds beter in staat om niet alleen informatie over de bron, maar ook over activiteiten af te leiden uit sporen, en daarmee scenario's over activiteiten te toetsen. Zonder andere opsporingsinformatie is het



Figuur 8: Het spanningsniveau van de batterij van de onderzochte iPhone 6s op een schaal (verticaal) van 0 tot 100% van 18 tot en met 23 november (horizontaal).

12. C.J. de Poot, *Wetenschap op de plaats delict*, Lectorale rede, Hogeschool van Amsterdam & Politieacademie 2011.

echter moeilijk om de complexe omstandigheden waarin de sporen zijn veroorzaakt te achterhalen, en om te bepalen in welke volgorde de sporen zijn ontstaan.[13,14]

In dat opzicht verschilt digitaal bewijs van fysiek bewijs. Zoals we lieten zien bevat digitaal bewijs vaak wel informatie over de precieze momenten in de tijd en de precieze volgorde waarin sporen zijn ontstaan. Daarnaast bevat digitaal bewijs soms communicatie-informatie waarmee niet alleen een activiteit (de communicatie tussen personen, of tussen mens en computer) maar ook de inhoud van die communicatie (de aard van een gesprek via chat of e-mail, of van de zoektermen die werden ingevuld) direct in de tijd kan worden geplaatst.

Digitaal bewijs kan daarom niet alleen goed helpen bij het beantwoorden van de wie-vraag, door te achterhalen welke gebruiker schuilging achter een e-mailadres, een user account of een telefoonnummer, maar biedt daarnaast een breed palet aan mogelijkheden waarmee naar antwoorden op de andere W-vragen kan worden gezocht. Bovenal biedt digitaal bewijs de mogelijkheid om die verschillende vragen over personen (wie), activiteiten (wat), plaats (waar) en tijd (wanneer) aan elkaar te verbinden en met elkaar in verband te brengen. Als het gaat om bewijs op activiteitniveau hebben digitale sporen dus een groot potentieel.

De voorbeelden die we gebruikten laten zien dat digitaal bewijs op activiteitniveau een belangrijke rol kan spelen nadat de verdachte bekend is, omdat de sporendragers in onze voorbeelden veelal afkomstig waren van de verdachten. Echter, ook in onderzoeken waarin gezocht wordt naar een onbekende verdachte kunnen digitale sporen een belangrijke rol spelen bij het vormen van scenario's. In die fase van het onderzoek zit de uitdaging vooral in het gericht zoeken naar sporen en sporendragers die mogelijk gerelateerd zijn aan het misdrijf. Sporendragers van slachtoffers en van apparaten op of in de omgeving van de plaats delict kunnen daarvoor worden gebruikt. In dat opzicht is er bij de meeste misdrijven geen groot verschil met de zoektocht naar andere informatie die gerelateerd kan worden aan de zaak. Nieuw is de rol die digitale sporen spelen bij het vormen en toetsen van scenario's bij verschillende vormen van cybercrime, die zich soms volledig afspelen in cyberspace, zoals het geval was in het onderzoek naar de computerinbraak bij Diginotar in 2011[15] en zeer recent de cyberaanval met ransomware bij Universiteit Maastricht.[16]

7. Tot slot

We lieten in dit artikel zien dat digitaal bewijs een schat aan informatie bevat waarmee strafbare feiten kunnen worden gereconstrueerd en kunnen worden bewezen. Digitale sporen zijn nu nog bij uitstek het werkveld van digitaal forensisch experts. Echter, om deze informatie goed te kunnen benutten in het opsporingsproces zullen andere specialisten in de forensische opsporing, rechercheurs, officieren van justitie, advocaten en rechters beter inzicht moeten krijgen in het werk van deskundigen op het gebied van digitaal forensisch onderzoek.[17] Daarnaast is een harmonisatie nodig tussen digitaal forensisch onderzoek en traditioneel forensisch onderzoek.[18] Digitale sporen zijn niet alleen waardevol bij het evalueren en opstellen van scenario's. Scenario's kunnen ook helpen om te bepalen welke digitale sporen uit het enorme aanbod aan mogelijk digitaal bewijs moeten worden veiliggesteld. Dat is van belang, omdat het praktisch onmogelijk is om alle digitale sporen die mensen tijdens hun activiteiten achterlaten te verzamelen en te onderzoeken.

De digitaal forensisch experts zullen zich op hun beurt moeten blijven ontwikkelen en leren om te denken en rapporteren op activiteitniveau waarbij samenwerking met de andere partijen in het opsporingsproces essentieel is. Inhoudelijk zullen experts de snelle ontwikkelingen op het gebied van (consumenten)elektronica en digitaal forensisch onderzoek moeten blijven volgen. Gelet op de grote hoeveelheid aan digitale sporen zullen de experts ook in staat moeten zijn met behulp van *data science* en data-visualisatietechnieken te zoeken naar verbanden en naar patronen in de activiteiten die relevant zijn voor het evalueren van een scenario. Het blijft overigens niet alleen bij het evalueren van scenario's. Bij digitale misdrijven (zoals het stelen van persoonlijke gegevens en het hacken van websites) kan het voorkomen dat experts scenario's moeten opstellen aan de hand van uitsluitend digitale sporen omdat het delict zich letterlijk onzichtbaar voor de buitenwereld heeft afgespeeld in cyberspace.

13. *Idem*.
14. C.J. de Poot, *De reconstructie van strafbare feiten*, Den Haag: Boom criminologie 2018.
15. H. Hoogstraten, 'Black Tulip Report of the investigation into the DigiNotar Certificate Authority breach', Augustus 2012, DOI 10.13140/2.1.2456.7364.
16. Rapport van Fox-IT met toelichting Universiteit Maastricht, '*UM Cyber Attack Symposium – Lessons learnt*', 2020, https://www.maastrichtuniversity.nl/um-cyber-attack-symposium---lessons-learnt.
17. H. Henseler & S. van Loenhout, 'Educating judges, prosecutors and lawyers in the use of digital forensic experts', *Digital Investigation*, Volume 24, Supplement, maart 2018, p. S76-S82.
18. M. Pollitt e.a., 'A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence', *OSAC Technical Series 0002*, 2018, https://www.nist.gov/system/files/documents/2018/01/10/osac_ts_0002.pdf.