IoT geeft digitale speurders veel meer bruikbare sporen

OP ZOEK NAAR HET DIGITALE SPOOR

De tientallen miljarden slimme apparaten en smartphones die nu al het internet of things (IoT) vormen, laten een enorme hoeveelheid digitale sporen na. Een deel daarvan is zeer bruikbaar voor forensisch onderzoek. Met behulp van datascience kunnen volgens Hans Henseler en Christianne de Poot veel betere analyses gedaan worden van die sporen; niet alleen op bronniveau maar ook op activiteitenniveau.

door Hans Henseler en Christianne de Poot beeld Shutterstock

Met de aanhoudende groei van IoT en ICT-netwerken komen meer data voorhanden die als digitale sporen kunnen dienen. De zoektocht naar het juiste digitale spoor vereist daardoor de inzet van datascience en datavisualisatie om scenario's te toetsen of aan te vullen. Soms moeten experts, indien het delict zich letterlijk onzichtbaar heeft afgespeeld in cyberspace, een scenario opstellen aan de hand van uitsluitend digitale sporen. Denk daarbij aan digitale misdrijven zoals phishing van persoonlijke gegevens, het hacken van bedrijfsnetwerken en aanvallen met ransomware. Het onderzoek van Fox-IT met een reconstructie van de recente cyberaanval op Universiteit Maastricht is daarvan een sprekend voorbeeld.

Sporen op de plaats delict 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.

SYMPOSIUM

Op 17 maart wordt het 11de E-Discovery Symposium georganiseerd door het lectoraat Digital Forensics & E-Discovery. Het thema van het symposium is dit jaar de betekenis van digitale sporen. Voor meer informatie en aanmelden: www.hsleiden.nl/digital-forensics/agenda/symposium/e-discovery-2020. In het tijdschrift Expertise & Recht wordt een uitgebreidere versie van dit artikel gepubliceerd.

BEWIJS OP BRONNIVEAU VERSUS ACTIVITEITENNIVEAU

Het analyseren van sporen op activiteitenniveau is relatief nieuw en vindt plaats bij onderzoek naar DNA, vezels, glas, verf, schotresten en vingersporen. Het verschil tussen bronniveau en activiteitenniveau kan uitgelegd worden aan de hand van een voorbeeld waarbij vingersporen op de plaats delict zijn aangetroffen.

Een vrouw belt de politie om een inbraak in haar appartement aan te geven. De politie vindt vier vingerafdrukken op de reling van het balkon, wat leidt tot de veronderstelling dat de dader het appartement via het balkon is binnengekomen. Door een match in een vingersporendatabase wordt een verdachte gevonden, die een bekende is van de vrouw.

De verdachte beweert dat hij niet via het balkon is binnengedrongen, maar dat hij een week eerder bij de vrouw op bezoek is geweest en een sigaret heeft gerookt op het balkon terwijl hij de reling vasthield.

In dit soort zaken wijzigt de centrale vraag van 'van wie zijn de vingerafdrukken?' naar 'welke activiteit leidde tot de sporen van de vingerafdrukken?', wat een geheel andere interpretatie van de bevindingen vereist. De aanwezigheid van de vingerafdrukken van de verdachte op het balkon wordt niet betwist, maar op welke wijze de vingerafdrukken daar terecht zijn gekomen.

Vaak moet daarvoor ook worden achterhaald door welke activiteit het spoor terecht is gekomen waar het werd aangetroffen.

Smartphones en slimme apparaten die verbonden zijn met het internet bevatten uiteenlopende digitale sporen die een schat aan informatie bevatten voor forensisch onderzoek (zie ook de publicatie 'AI helpt rechercheur zoeken naar digitale sporen', AG Connect, april 2019). Dit jaar zullen naar verwachting zo'n 20 tot 30 miljard objecten met elkaar verbonden zijn in het IoT.

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 (zie ook de publicatie 'De revolutie van digitaal bewijs', AG Connect, oktober 2017). 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 kunstmatige

‘Digitale sporen hebben groot potentieel op activiteitenniveau’

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. In de huidige rechtspraak zijn voldoende voorbeelden te vinden die 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. Uit verklaringen van slachtoffers en getuigen kunnen soms complete scenario’s over wat er is gebeurd worden gereconstrueerd.

DIGITAAL BEWIJS IN STRAFZAKEN

Op rechtspraak.nl wordt informatie gepubliceerd over onder andere uitspraken van de rechtspraak. Aan de hand van drie verschillende uitspraken proberen we een beeld te schetsen hoe digitaal bewijs in het strafrecht wordt gebruikt. Het betreft de moord op Koen Everink, de moord op de Bûterwei en een uitspraak in een strafzaak over het bezit van kinderpornografisch materiaal.

Bij de moord op Koen Everink werd de verdachte geconfronteerd met belastende zoektermen die waren aangetroffen in de zoekgeschiedenis op zijn iPad. De verdediging voerde als verweer aan dat de verdachte sommige belastende zoektermen niet zelf had ingevuld en betwiste het tijdstip van de andere zoekvragen. Ook waren gegevens uit de stappenteller op de telefoon van de verdachte in strijd met zijn alibi.

De doorbraak in het onderzoek naar de moord op de Bûterwei kwam pas nadat de in de Google-cloud opgeslagen activiteit van de verdachte (en vrouw van het slachtoffer) werd onderzocht. Toen de verdachte ondervraagd werd, bleken diverse verklaringen onwaar te zijn op basis van het digitaal bewijs dat in de telefoon van de verdachte en van het slachtoffer werd gevonden.

Bij veel zaken waarin de verdachte het bezit van kinderpornografisch materiaal ten laste is gelegd, is een computer in beslag genomen waarop belastende foto’s en of video’s zijn aangetroffen. De verdachte betwist dit niet maar verdedigt zich door te verklaren dat hij niet wist dat die bestanden op zijn computer stonden. Vaak kan aan de hand van activiteit op de computer worden aangetoond dat er wel degelijk opzet was en ook dat de verdachte gedurende langere periodes stelselmatig heeft gezocht naar soortgelijk materiaal.

DIGITAL WELLBEING EN SCREEN TIME

In 2018 is zowel Apple als Google begonnen met het toevoegen van zogenaamde time trackers op hun telefoons. Google noemt deze functionaliteit Digital Wellbeing 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 hoelang en wanneer 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 van apps wordt geregistreerd. Digitaal forensisch onderzoekers hebben uitgepluisd in welke bestanden en in welk formaat deze eigenschappen worden opgeslagen. Zo houdt Apple in iOS de administratie bij in de KnowledgeC-tabellen, waarover wordt gerapporteerd door onafhankelijk onderzoekers maar ook door ontwikkelaars van commerciële tools.

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 de zaak van Koen Everink 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 het ene scenario waarschijnlijker is dan het andere scenario.

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

‘Digitaal bewijs kan inhoud van communicatie direct in de tijd plaatsen’

In dat opzicht verschilt digitaal bewijs van fysiek bewijs. Digitaal bewijs bevat 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 het gesprek, 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 andere opsporingsvragen kan worden gezocht. Bovenal biedt digitaal bewijs de mogelijkheden 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 activiteitenniveau hebben digitale sporen dus een groot potentieel.

REACTIES EN BIJDRAGEN

Voor reacties en nieuwe bijdragen van IT-experts:
Tanja de Vrede
020-2356415
t.d.vrede@agconnect.nl

AUTEURS

DR. IR. HANS HENSELER
is lector Digital Forensics & E-Discovery bij de specialisatie Forensische ICT aan de Hogeschool Leiden. (henseler.h@hsleiden.nl).

PROF.DR. CHRISTIANNE DE POOT
is hoogleraar Criminalistiek aan de Vrije Universiteit. Tevens is zij lector Forensisch Onderzoek bij de Hogeschool van Amsterdam en Politieacademie.