Steeds vaker worden sociale media geografisch gefilterd en automatisch geanalyseerd

EXPONENTIËLE GROEI DIGITAAL BEWIJS

Als drager van digitaal bewijs heeft de smartphone de computer ruimschoots ingehaald. E-Discovery staat aan het begin van een nieuw tijdperk, zegt Hans Henseler, doordat digitale sporen nu aan personen en locaties te koppelen zijn. Digitale sporen krijgen het karakter van klassieke forensische sporen zoals vingerafdrukken en voetsporen.

door: HANS HENSELER

De exponentiële groei van digitaal bewijs in forensisch digitaal onderzoek in de opsporing en in interne bedrijfsonderzoeken zet, zoals verwacht, door. Niet alleen de omvang van het bewijs neemt toe, ook de plaatsen waar digitale sporen te vinden zijn, veranderen snel. De afgelopen jaren heeft de smartphone als drager van digitaal bewijs de computer al ruimschoots ingehaald. Tegenwoordig zien we dat de digitale sporen zich van onze mobile devices naar de cloud verplaatsen. Onze computers, tablets en smartphones zijn in feite toegangspoorten geworden tot onlineomgevingen in publieke of hybride cloudomgevingen. Zij bevatten nog wel restanten van sporen maar het wordt steeds lastiger om feiten te reconstrueren aan de hand van slechts één device. Tegelijkertijd maken zowel opsporingsdiensten als bedrijven meer en meer gebruik van onderzoeken in online media. Denk aan het monitoren van productacceptatie, populariteit van tv-programma's tot en met het monitoren van sentimenten die gerelateerd zijn aan beursgenoteerde ondernemingen. Steeds vaker ook worden sociale media geografisch gefilterd en automatisch geanalyseerd om snel te kunnen reageren op incidenten. Voor maatschappelijke veiligheid kunnen sociale media een welkome aanvulling zijn op het blauw op straat. Dan kan het gaan om foto- en videomateriaal op locaties of om het volgen van grote stromen mensen bij evenementen zoals bijvoorbeeld Koningsdag in Amsterdam.

The Decade of Discovery

De documentaire 'The Decade of Discovery' schetst hoe E-Discovery zich heeft ontwikkeld in de periode van circa 2002 tot 2012. In 2002 ontstonden de eerste E-Discovery-problemen toen de toenmalige president van de VS Bill Clinton aankondigde dat de overheid de tabaksindustrie zou gaan vervolgen om de alsmaar stijgende ziektekosten van patiënten met longkanker op de tabaksindustrie te verhalen. Bij de National Archives realiseerde men zich dat het onmogelijk was om alle beschikbare e-mails door te lezen. Het filteren van e-mails op trefwoorden was noodzakelijk om de review beheersbaar te houden. Met de explosieve groei van informatie bleken telkens nieuwere technologieën nodig te zijn. Daarbij was niet altijd de techniek het probleem maar wel de acceptatie van wat technisch al langer mogelijk was. Alhoewel de film voornamelijk is geïnspireerd door de E-Discovery-praktijk in de VS zijn veel van de problemen, en de oplossingen, relevant voor de toepassing van E-Discovery in Europa en in Nederland.

Clouddiensten

De combinatie van smartphones met clouddiensten is interessant voor onderzoekers. Smartphones zijn in hoge mate gebonden aan een persoon en door het contact met de cloud wordt veel vaker dan voorheen de locatie van de smartphone en dus van de gebruiker vastgelegd. Tot voor kort was E-Discovery vooral gericht op het analyseren van documenten om te achterhalen wie wat wist en wanneer. Nu is het ook mogelijk om te bepalen waar de gebruiker zich bevond. Daarmee komen de digitale sporen langzaam meer op het terrein van de klassieke forensische sporen zoals vingerafdrukken, voetsporen en de relatief nieuwe DNA-sporen.
Terugkijkend was onderzoek naar E-Discovery tot nu toe vooral gericht op information retrieval. De centrale vraag was gericht op het vinden van technieken waarmee partijen in een conflict op afdoende wijze relevante e-mails en documenten kunnen produceren. Deze geschiedenis wordt beschreven in de documentaire The Decade of Discovery (zie kader). De film schetst hoe op dit moment technology assisted review een geaccepteerde benadering is geworden waarmee we de alsmaar groeiende stroom aan digitaal bewijs kunnen beheersen. Een van de lessen die de documentaire ons leert is dat advocaten en rechters hebben ingezien dat mensen niet zulke betrouwbare reviewers zijn. Het bepalen van relevantie is lastig en, zoals Doug Oard van de University of Maryland in de documentaire uitlegt, kan relevantie pas definitief bepaald worden nadat alle informatie is verwerkt. De belangrijkste doorbraak is daarom misschien ook niet dat advocaten en rechters nu accepteren dat computers reviewen maar dat ze accepteren dat je met steekproeven heel goed de betrouwbaarheid van een reviewproces kunt meten. Of dit nu een review is door mensen of door computers.

Nieuw tijdperk

Op dit moment staat het onderzoek naar E-Discovery aan het begin van een nieuw tijdperk doordat digitale sporen nu aan personen en locaties te koppelen zijn (zie kader). Politie-, veiligheids- en bijzondere opsporingsdiensten konden al langere tijd gebruik maken van plaatsbepaling van telefoons door informatie bij de mobiele telefoonproviders op te vragen. Deze informatie is in de praktijk niet altijd betrouwbaar en het opvragen van informatie bij providers is gebonden aan strenge voorwaarden. Smartphones houden nu zelf de locatie bij (vaak op meer dan één manier: zie kader). Van een telefoon die als bewijs in beslag is genomen, kan betrouwbaarder en ook zonder aanvullende rechtsverzoeken vastgesteld worden waar die is geweest. Zelfs tablets en notebooks die geen mobiele telefoonverbinding hebben maar wel een wifi-verbinding, zijn tegenwoordig in staat om hun eigen positie te bepalen (zie kader).
Met de integratie van mobiele devices en clouddiensten worden de digitale sporen ook vluchtiger. Na verloop van tijd verdwijnen ze automatisch van het apparaat en de gebruiker kan ze later altijd weer via een onlineverbinding raadplegen. Natuurlijk zijn ook vluchtige sporen terug te vinden met forensische methoden totdat de data overschreven worden in het geheugen. In dat geval is er echter altijd nog de online informatie beschikbaar. Het onderzoek van online en devicedata zal geïntegreerd worden. Onderzoekers hebben behoefte aan nieuwe technieken waarmee ze digitale sporen uit devices kunnen verrijken met digitale sporen uit sociale media en vice versa.
Voor open bronnen zoals Twitter is dit geen probleem maar voor meer gesloten bronnen zoals Dropbox, Whatsapp, Facebook, Linked-In et cetera, zal er vermoedelijk nieuwe wetgeving nodig zijn. In de tijd dat een mobiele telefoon alleen gebruikt werd om te bellen en slechts de laatste tien oproepen werden onthouden, vond men het gerechtvaardigd om die telefoon in beslag te nemen en te onderzoeken. Tegenwoordig vangt men bij een inbeslaggenomen computer of smartphone alle zakelijke en privégegevens van de afgelopen jaren. Partijen, inclusief de wetgever, vragen zich terecht af of al dat bewijs wel geanalyseerd mag worden terwijl het een verdenking betreft die een veel beperktere reikwijdte van het onderzoek rechtvaardigt. «

SYMPOSIUM E-DISCOVERY

Het Symposium E-Discovery in Nederland wordt dit jaar voor de zesde maal georganiseerd door het lectoraat E-Discovery van de Hogeschool van Amsterdam in Pakhuis de Zwijger op 23 april aanstaande. Op het symposium zal Jason Baron spreken. Hij sprak ook op het symposium in 2011 en speelt de hoofdrol in The Decade of Discovery. Jason zal de film inleiden en deelnemen aan het discussiepanel dat aansluitend wordt gehouden. Geert Lovink van het Instituut van Network Cultures van de Hogeschool van Amsterdam zal aandacht besteden aan strategieën van klokkenluiders waarbij Snowden en Wikileaks als voorbeeld worden gebruikt. Arnout de Vries van TNO legt uit waarom hij denkt dat de sociale media gezien moeten worden als het nieuwe DNA en zullen zorgen voor een nieuwe revolutie in de opsporing. John Jansen van Pagefreezer betoogt dat alles wat op het web te vinden is, onweerlegbaar bewijs is. Voor meer informatie: http://ediscoverynl.dmci.hva.nl.

LOCATIEBEPALING MOBIELE APPARATUUR

Voor de locatiebepaling van smartphones en tablets (en computers met een wifi-aansluiting) zijn een aantal methoden voorhanden. De eerste methode is de plaatsbepaling aan de hand van zendmastgegevens (als het apparaat met het mobiele telefoonnet verbonden is geweest). Deze gegevens kunnen door de provider worden aangeleverd. De nauwkeurigheid laat echter te wensen over. Door weersomstandigheden, reflecties van grote gebouwen en door drukte op het netwerk is er geen garantie dat een telefoon altijd met de dichtstbijzijnde zendmast verbinding heeft. De tweede methode is door de GPS-locaties die in het apparaat zijn opgeslagen, uit te lezen. De frequentie en de duur van de opslag worden bepaald door de applicaties op de telefoon.
De derde methode is door het uitlezen van zendmast (cell) id's of wifi-netwerken in het geheugen van het apparaat. Op internet zijn databases te vinden die de locaties bijhouden van alle bekende zendmasten. Plaatsbepaling aan de hand van wifi-netwerken is iets lastiger, maar zowel Google als Apple bieden diensten aan om, bij slechte GPS-ontvangst, toch redelijk nauwkeurig de locatie te bepalen aan de hand van omringende wifi-netwerken.

Hans Henseler is lector E-Discovery in het Kenniscentrum Create-IT van de Hogeschool van Amsterdam en directeur en mede-oprichter van het bedrijf Tracks Inspector. Hij zal op het symposium van 23 april a.s. spreken over ontwikkelingen in Semantic Search voor E-Discovery.

ag
Voor reacties en nieuwe bijdragen van IT-experts:
Henk Ester,
070 3046812
h.ester@automatiseringgids.nl