DR. IR. J. HENSELER

E-Discovery

Op zoek naar de digitale waarheid

Hogeschool van Amsterdam

E-Discovery

Op zoek naar de digitale waarheid

Openbare Les

uitgesproken op woensdag 14 april 2010

door

Dr. ir. J. Henseler

Lector E-Discovery aan de Hogeschool van Amsterdam

HVA PUBLICATIES

HvA Publicaties is een imprint van Amsterdam University Press.
Deze uitgave is totstandgekomen onder auspiciën van de Hogeschool van Amsterdam.

Omslagillustratie: *Handen*, Pieter Schunselaar, fotocollectie Hogeschool van Amsterdam
Vormgeving omslag: Kok Korpershoek, Amsterdam
Opmaak binnenwerk: JAPES, Amsterdam

ISBN 978 90 5629 622 3
e-ISBN 978 90 4851 265 2

1. Inleiding

De rol van ICT wordt steeds belangrijker in ons maatschappelijke en economische verkeer. Voor de meest eenvoudige handelingen wordt tegenwoordig wel gebruikgemaakt van één of meer ICT-toepassingen. Zijn de zegeningen van ICT groot, tegelijkertijd brengt deze ontwikkeling ook bijzondere risico's met zich mee. Als er iets misgaat, per ongeluk of met opzet, stelt dat bijzondere eisen aan het onderzoek naar de toedracht. Digitale sporen moeten kunnen worden getraceerd en geanalyseerd, en moeten worden bewaard en gepresenteerd op een manier die enerzijds praktisch haalbaar is en anderzijds tegemoetkomt aan wat de wet bij sporen voorschrijft om als wettelijk bewijsmateriaal te dienen. Dit omvangrijke werkterrein, dat nog volop in ontwikkeling is, wordt aangeduid met E-Discovery.

Bij E-Discovery gaat het erom dat informatie op forensisch verantwoorde wijze veiliggesteld én slim verwerkt wordt. Zo wordt bij het onderzoek naar geruchtmakende miljardenfraudes als die van Stanford en Madoff ruimschoots gebruikgemaakt van digitale opsporings- en bewaartechnieken. Maar ook bij minder opzienbarende faillissementen wordt ernaar teruggegrepen om eventuele fraudes te kunnen aantonen. Bedrijven en instellingen doen ook veelvuldig een beroep op zulke bijzondere opsporingstechnieken om hen te helpen bij interne onderzoeken.

Met het Lectoraat E-Discovery wil de Hogeschool van Amsterdam het onderwijs op dit specifieke terrein verbeteren, en tegelijkertijd de kennis- en expertise-uitwisseling naar een hoger niveau tillen. Daartoe wordt een voor alle betrokken partijen (binnen zowel de overheid als het bedrijfsleven) toegankelijk expertisecentrum opgezet in de vorm van een Kenniskring waarin wordt samengewerkt met andere deskundigen. De expertise van de Kenniskring beperkt zich niet tot het ontwikkelen van en adviseren over methoden en technieken voor digitaal opsporen, maar richt zich ook op de ontwikkeling van een kader voor 'forensic readiness': het preventief verzamelen van tegenbewijs en het klaar zijn voor forensische onderzoeken.

In deze openbare les wil ik het onderwerp E-Discovery vanuit verschillende perspectieven belichten om uiteindelijk tot een onderzoeksagenda van het lectoraat te komen, die aansluit bij het Domein Media, Creatie en Informatie en een zinvolle bijdrage levert aan de ontwikkeling van het vakgebied E-Discovery.

2. Het belang van de digitale waarheid

Voordat ik dieper inga op het onderwerp E-Discovery, wil ik hier eerst ingaan op het toenemende belang van de digitale waarheid in onze hedendaagse digitale samenleving. Het begrip digitale waarheid is een verwijzing naar waarheidsvinding op grond van digitale sporen die aangetroffen worden in een geautomatiseerde omgeving, elektronische gegevensdragers enzovoorts. Om dat belang te kunnen begrijpen is het nodig de ontwikkelingen op het terrein van de digitale waarheidsvinding te beschrijven. In Nederland lijken die ontwikkelingen ongeveer te beginnen eind jaren '80 van de vorige eeuw, en daarom zullen we ons in dit geval beperken tot de ontwikkelingen in Nederland in de afgelopen twintig jaar. Die twintig jaar is overigens niet zo gek als we bedenken dat de hele ICT-revolutie nog geen vijftig jaar geleden is begonnen.

De technische ontwikkelingen illustreren de snel veranderende mogelijkheden van ICT, maar zeggen op zich niet veel over het belang van de digitale waarheid. In de jaren '90 was het zoeken in digitale sporen vooral in opkomst bij politie en bijzondere opsporingsdiensten, als onderdeel van het forensisch computeronderzoek (Henseler, 1994). In het begin van de 21ste eeuw zien we dat elektronische informatie steeds belangrijker wordt. Daardoor wordt als gevolg van economische criminaliteit de digitale waarheid uiteindelijk in grootschalige (interne en externe) onderzoeken ook belangrijker voor bedrijven.

2.1 Technische ontwikkelingen in de afgelopen twintig jaar

Eind jaren '80 wordt langzaam duidelijk dat het zoeken naar digitale sporen noodzakelijk is in het verlengde van het normale forensische onderzoek. De nadruk ligt dan nog vooral op computercriminaliteit en computerbeveiliging. Dit komt in eerste instantie vooral tot uiting in het onderzoek bij politie en justitie, die in toenemende mate geconfronteerd worden met digitale sporen. Als de politie en bijzondere opsporingsdiensten in Nederland begin jaren '90 speciale teams computercriminaliteit oprichten, kan het toenmalig Gerechtelijk Laboratorium niet achterblijven, en het gaat op zoek naar een forensisch computeronderzoeker. Die begint in februari 1992 als medewerker van de afdeling schriftonderzoek. De daaropvolgende jaren vindt een gecoördineerde groei plaats van zowel de derde lijn (Gerechtelijk Laboratorium en Centrale Recherche Informatiedienst) als de tweede lijn (teams computercriminaliteit van onder andere politie, Agrarische Inlichtingen Dienst AID, Fiscale Inlichtingen en Opsporingsdienst FIOD en de destijds nog aparte Economische Controle Dienst ECD).

Forensisch computeronderzoek bij het Gerechtelijk Laboratorium

Het Gerechtelijk Laboratorium (GL) van het Ministerie van Justitie heet tegenwoordig het Nederlands Forensisch Instituut (NFI). De afdeling Schriftonderzoek doet forensisch onderzoek naar handschrift en machineschrift in het kader van de waarheidsvinding. Een forensisch schrijfmachineonderzoeker vergelijkt bijvoorbeeld een brief met de eigenschappen van een schrijfmachine om sporen te vinden waaruit afgeleid kan worden of de brief met die schrijfmachine is getypt. Dat kan bijvoorbeeld op grond van kleine beschadigingen in de letterstempels, of door de doorslag op het typelint te vergelijken met de tekst in de brief. Deze onderzoeksmethode wordt ook toegepast op brieven en elektronische printers die ter onderzoek worden aangeboden. Als echter met de printers ook de bijbehorende computers ter onderzoek worden aangeboden, ligt het voor de hand om de elektronische inhoud van brieven terug te vinden op de harde schijf of gegevensdragers die bij die computer horen. Dit was in feite de aanleiding voor mijn aanstelling als forensisch computeronderzoeker in 1992. Daarmee was de basis gelegd voor de groep forensisch computeronderzoek, die toen nog onderdeel uitmaakte van de afdeling forensisch schriftonderzoek.

Criminelen in Nederland bleken toen al veel gebruik te maken van elektronische zakagenda's om daar belangrijke informatie in op te slaan en die te beveiligen met een wachtwoord. Mede daardoor groeide het aantal zaken van 58 in 1992 naar 120 in 1994 (Henseler, 1994). Voor de politie waren elektronische zakagenda's toen een veelvoorkomend probleem. Voordat het GL de mogelijkheid had om elektronische zakagenda's te kraken, moesten rechercheurs regelmatig met een internationaal rechtshulpverzoek op zak in het vliegtuig naar de fabrieken van Casio of Sharp in Japan. Nadat de eerste modellen bij het GL gekraakt konden worden, ontstond er een nauwe samenwerking met de afdeling computercriminaliteit van de Centrale Recherche Informatiedienst (CRI), en gezamenlijk werden de toenmalige teams computercriminaliteit van de politie ondersteund. In 1993 lanceerde het Ministerie van Justitie onder minister Hirsch Ballin het project 'Aanpak van de Zware, Georganiseerde Criminaliteit'. In dat verband wist het GL aanvullend budget te krijgen om slimme tools te maken. Met die tools konden de teams computercriminaliteit van de politie zelf elektronische zakagenda's kraken en uitlezen. Ondertussen konden de onderzoekers op het GL methoden ontwikkelen voor de nieuwe modellen die in hoog tempo door Sharp en Casio op de markt werden geïntroduceerd. Dit project was bijzonder succesvol en de groep groeide in 1994 tot een zelfstandige afdeling met vijf onderzoekers.

In 1995 herhaalde deze geschiedenis zich. Het ging toen niet om elektronische zakagenda's, maar om versleuteling van digitale gegevens door criminelen, waardoor waarheidsvinding en opsporing ernstig gehinderd dreigden te worden. De afdeling groeide naar 26 medewerkers in 1996. Door de groeiende complexiteit werden verschillende deskundigheidsgebieden geïdentificeerd, namelijk onderzoek naar gesloten systemen, naar open systemen en naar communicatie (Henseler, 2000). Niet alleen het toegankelijk maken van versleutelde informatie bleek een probleem. De snelle technische ontwikkeling van datacommunicatie met de toenmalige high-speed modems en de introductie van het GSM-netwerk introduceerden een waaier van technische problemen, die justitie en politie in het kader van wetgeving en opsporing voor grote uitdagingen stelden. De specialisten van het GL hebben sindsdien ook op deze terreinen een belangrijke adviserende rol.

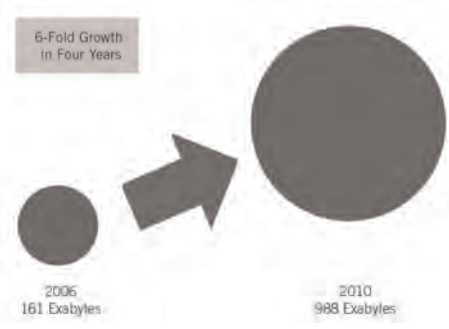
De afdeling forensisch computeronderzoek is uitgegroeid tot de bredere afdeling Digitale Techniek en Biometrie. Die telt momenteel veel deskundigheidsgebieden en heeft in totaal ongeveer honderd onderzoekers. De kwaliteit van het onderzoek en de onderzoekers staat internationaal zeer hoog aangeschreven. Een aantal onderzoekers uit 1996 werkt nog steeds bij de afdeling terwijl anderen hun werkzaamheden hebben voortgezet bij opsporings- en inlichtingendiensten of in het bedrijfsleven.

Bij opsporingsdiensten ligt in die periode de nadruk op forensisch computeronderzoek van elektronische zakagenda's, mobiele telefoons en semafoons, die begin jaren '90 hun intrede doen en vooral bij de georganiseerde criminaliteit zeer gewild zijn (Henseler, 1994). Hoewel de problemen in technisch opzicht uitdagend zijn te noemen, vallen de hoeveelheden informatie in die tijd nog mee en kunnen adres- en bankgegevens eenvoudig geprint worden. Het faxverkeer overheerst dan nog, en bijvoorbeeld het uitlezen van faxberichten in het geheugen van modernere faxapparaten wordt belangrijk.

E-mail wordt in de eerste helft van de jaren '90 door het Nederlandse bedrijfsleven nog maar mondjesmaat gebruikt en ook internet speelt een beperkte rol. Dat verandert in de tweede helft van de jaren '90, naarmate de prijs-prestatieverhouding van computers en internettoegang verbetert. Bekende e-mailoplossingen, zoals IBM Lotus Notes, Novell Groupwise en Microsoft Exchange Server, worden langzaam gemeengoed in bedrijven, en nieuwe versies van deze werkgroepprogramma's bieden gebruikers, naast de mogelijkheid om e-mails te versturen, ook elektronische kalenders waarin medewerkers

hun eigen agenda kunnen bijhouden en vergaderverzoeken kunnen rondsturen. Eind jaren '90 gaan de ontwikkelingen op internet zelfs zo snel dat de economie oververhit raakt, en we belanden in 2001 in een recessie nadat de zogenaamde internetbubbel in 2000 uit elkaar is gespat.

Niet alleen het aantal gebruikers van e-mail en andere nieuwe vormen van digitale communicatie neemt toe, ook de capaciteit van (persoonlijke) opslagmedia groeit exponentieel. De opslagcapaciteit van diskruimte is de afgelopen twintig jaar nog sneller toegenomen dan we volgens de Wet van Moore zouden mogen verwachten (Moore, 1965). Terwijl de Wet van Moore stelt dat het aantal transistors op een IC (Integrated Circuit, een chip) iedere twintig maanden verdubbelt, geldt in ieder geval voor de periode 1995-2005 de Wet van Kryder[1], die stelt dat opslagcapaciteit van harde schijven nog sneller verdubbelt dan het aantal transistors volgens de Wet van Moore. Door die exponentiële groei krijgen we, zoals iedereen zelf kan beamen, na al die jaren de beschikking over computers met een enorme opslagcapaciteit. De gemiddelde harddisk-omvang is veel sneller toegenomen dan de gemiddelde documentgrootte. Tot begin jaren 2000 zaten onze harde schijven sneller vol. Gebruikers zagen zich genoodzaakt regelmatig elektronische informatie te archiveren om voldoende vrije werkruimte beschikbaar te houden. Het gebruik van verwisselbare media zoals diskettes, CD's en ZIP drives beleefde een hoogtepunt. Tegenwoordig speelt dit probleem minder en lijkt de hoeveelheid beschikbare diskruimte onbegrensd.



Figuur 1: Groei van digitale informatie 2006-2010 (IDC, 2007)

Maar al blijft de groei van de gemiddelde documentomvang achter bij de exponentiële groei van opslagcapaciteit, toch voorspelt industrie-analist IDC dat we in 2010 zesmaal zoveel digitale informatie hebben als in 2006. Dit wordt geïllustreerd in figuur 1, waarin IDC de hoeveel informatie die gemaakt, vastgelegd en gekopieerd is, schat op 161 exabytes (1 exabyte = 1 miljoen terabyte).

De verwachting is dat deze hoeveelheid informatie in 2010 is toegenomen tot 988 exabytes, bijna 1 zettabyte. Die groei laat zich verklaren door de toename van omvangrijkere multimediabestanden, zoals geluid, foto's en video, door het groeiende aantal computergebruikers, maar vooral ook doordat bedrijven steeds meer bedrijfsprocessen inrichten rondom digitale informatie.

2.2 Het groeiende belang van elektronische informatie

Tegelijk met de hiervoor geschetste technische ontwikkelingen valt waar te nemen dat elektronische informatie niet alleen bij criminelen een steeds grotere rol gaat spelen, maar ook in het economische verkeer. Door die ontwikkeling is het onvermijdelijk dat elektronische informatie steeds belangrijker wordt in de bedrijfsvoering en uiteindelijk ook bij het onderzoeken van economische criminaliteit. Voordat ik dieper zal ingaan op de rol van elektronische informatie in het kader van economische criminaliteit, schets ik eerst het belang van elektronische informatie aan de hand van nieuwe wet- en regelgeving voor bedrijven.

Enron was op het hoogtepunt van de internetbubbel eind jaren '90 een veelbelovend Amerikaans energiebedrijf dat in nieuwe technologieën investeerde en enorm goed presteerde op de beurs. Toch ging het mis. Bij een poging het bedrijf te redden kwam in november 2001 een grootschalige fraude met de boekhouding aan het licht. In december 2001 leidde dit tot het inmiddels beruchte faillissement (Fox, 2003). Dit leek in eerste instantie een typisch Amerikaanse aangelegenheid, maar een paar jaar later, in 2003, had Nederland haar eigen boekhoudschandaal met Ahold. Ten onrechte was omzet van buitenlandse dochterondernemingen meegenomen in de concernomzet. Het bedrog kon jarenlang worden volgehouden omdat men zogenaamde 'control letters' had opgesteld waaruit zeggenschap zou blijken, ondanks dat Ahold geen meerderheidsbelang had in deze ondernemingen. Deze zeggenschap werd echter ontkracht via 'side letters' die werden achtergehouden.

In 2002 kwam de zogenaamde Sarbanes Oxley-wet (SOx) tot stand in de VS. Die wet kwam er pas toen na Enron in 2002 Worldcom failliet ging, nadat ook daar een omvangrijk boekhoudschandaal aan het licht was gekomen. Met de SOx-wetgeving wordt nadrukkelijk geprobeerd om bedrijven ertoe te bewegen hun corporate governance te verbeteren, zodat ze transparanter worden in hun bedrijfsvoering, teneinde schandalen als Enron en Worldcom te voorkomen. Informatietechnologie vormt een belangrijk onderdeel van die corporate governance en bedrijven worden geacht duidelijke (interne) regels te volgen als het gaat om de archivering (en vernietiging) van bedrijfsinformatie, de zogenaamde 'records'. Hiermee wordt een opleving ingeluid van records management.

Records management

Door strengere compliance-eisen worden bedrijven zich (gedwongen) bewust van het feit dat elektronische berichtuitwisseling (e-mail) onderdeel uitmaakt van de bedrijfsvoering en dat zulke berichten net als schriftelijke correspondentie een belangrijke rol spelen. Tegenwoordig kunnen elektronische documenten en e-mailberichten een belangrijke sleutel zijn voor het leveren van bewijs in bijvoorbeeld een intern fraudeonderzoek, maar ook in een extern opgelegd onderzoek. Nieuwe regelgeving verbiedt het zonder meer verwijderen van digitale informatie die mogelijk als bewijs kan gebruikt worden (De Pous, 2007).

Echter, het niet mogen weggooien van digitaal bewijs is niet het voornaamste probleem. Door deze nieuwe regels wordt het voor alle bedrijven belangrijk om te weten welke elektronische data ze in huis hebben, op welke manier die beschikbaar is en vooral ook wanneer die informatie weggegooid moet worden! Want als het bedrijf kan aantonen dat e-mail volgens van tevoren gestelde regels is weggegooid, is dit nog steeds toegestaan (zolang er nog geen sprake is van een onderzoek).

Het identificeren van belangrijke bedrijfsgegevens en het vervolgens bewaren en vernietigen (de retentie) van die informatie heet records management. Dat is gericht op het beheer van informatie uit bedrijfsprocessen door documentaire informatieverzorgers (DIV'ers), tegenwoordig ook wel records managers genoemd. In overheidsorganisaties zorgt een DIV'er voor het beheer van informatie waar een bewaarplicht voor geldt. Dit vereist een strak regime dat zorgvuldig bijgehouden moet worden. DIV'ers krijgen een speciale opleiding om informatie op de juiste wijze te archiveren. Maar hoe zit dat nu met e-mail? In de praktijk weten werknemers in veel gevallen al niet eens waar of hoe ze hun e-mail moeten bewaren, laat staan dat ze weten wanneer ze e-mail mogen (of moeten) vernietigen.

Door de eerder geschetste informatie-explosie is records management niet langer een zaak van grote bedrijven of overheidsorganisaties. Ook kleine bedrijven hebben te maken met grote hoeveelheden informatie. Doordat digitale informatie zo gemakkelijk vermenigvuldigd kan worden is er veel informatie dubbel aanwezig en hoeft niet alles bewaard te worden. Maar voor het verwijderen van records zijn wel duidelijke regels nodig. Zonder zulke regels is het gevaar groot dat persoonlijke e-mailarchieven en back-up tapes onverwacht belastende informatie voor een bedrijf kunnen opleveren. Bovendien is het onderzoek ervan erg kostbaar.

Terwijl toezichthouders bedrijven steeds meer op de vingers kijken als het gaat om de wijze waarop ze omgaan met belangrijke elektronische bedrijfsinformatie, introduceren de VS eind 2006 een nieuwe versie van de Federal Rules of Civil Procedure (FRCP). De FRCP bevatten regels die van toepassing zijn op civiele rechtszaken die zich afspelen in de VS.[2] Deze regels bepalen onder andere welke plichten partijen hebben in de fase voorafgaand aan de rechtszaak waarin beide partijen documenten en ander bewijsmateriaal van elkaar kunnen vorderen. De nieuwe versie van de FRCP verwacht ten aanzien van potentieel elektronisch bewijs, dat alle bedrijven (en dus niet alleen beursgenoteerde bedrijven) richtlijnen hebben voor het bewaren en vernietigen van elektronische informatie, en weten hoe toegankelijk die gegevens zijn (inclusief gegevens in back-up systemen). Bovendien moeten die richtlijnen er rekening mee houden dat elektronische informatie niet vernietigd mag worden op het moment dat deze mogelijk relevant is voor een ingesteld onderzoek.

Ook in Nederland laten toezichthouders zich niet onberoerd als het gaat om het verzamelen van digitale informatie. Zo publiceerde de Nederlandse Mededingingsautoriteit (NMa) in 2003 in de *Staatscourant* van 11 juni 2003 haar 'Werkwijze m.b.t. het inzien en kopiëren van digitale gegevens en bescheiden' (die overigens in 2007 herzien is).[3] In 2006 publiceerde de Autoriteit Financiele Markten (AFM) een zelfde soort document.

Digitale werkwijze van de NMa

Al sinds 2003 hanteert de NMa een digitale werkwijze, die in 2007 door 'voortschrijdend inzicht en voorliggende jurisprudentie' werd aangescherpt. In grote lijnen komt het erop neer dat de NMa digitale kopieën van deelverzamelingen data maakt, of ervoor kan kiezen (afhankelijk van de toegankelijkheid van de beschikbare data en het doel van het onderzoek) om forensische images te maken. Gebeurt dat laatste, dan wordt feitelijk van alles wat op een computer is opgeslagen (inclusief besturingssoftware) een onderzoekskopie gemaakt. Maar dat levert een groot juridisch vraagstuk op; naast het feit dat ook gegevens die niet relevant zijn voor het onderzoek worden meegenomen, wordt zo ook beslag gelegd op privacygevoelige gegevens en geprivilegieerde informatie (alleen bestemd voor vertrouwelijke communicatie tussen de onderzochte rechtspersoon en zijn juridische vertegenwoordigers).

Om bedrijven de kans te geven om deze data terug te claimen, hanteert de NMa in haar digitale werkwijze een lockup-periode van tien dagen. Gedocumenteerde en goed onderbouwde claims binnen die periode worden gehonoreerd en de bewuste informatie wordt (zonder door NMa-functio-

narissen te zijn ingezien) verwijderd uit het onderzoeksmateriaal. Ook al lijkt deze werkwijze waterdicht, het blijft moeilijk om de juridisch geschoolde achterdocht van mededingingsspecialisten geheel weg te nemen. Hoewel de NMa met haar digitale werkwijze internationaal voorop loopt, blijven specialisten in Nederland erop hameren dat er naar hun mening onvoldoende waarborgen zijn. Hoe weten ze zeker dat de NMa zich bij het doorzoeken en rangschikken van het materiaal beperkt tot het vooraf aangegeven onderzoeksonderwerp? Ook wordt de termijn van tien dagen te kort gevonden, gezien de emotionele schok om onderwerp van een NMa-onderzoek te zijn én omdat de enorme omvang en complexiteit van de opgevraagde informatie meer voorbereidingstijd vragen.

Een ander discussiepunt betreft het feit dat de NMa in beginsel niet zelf digitale kopieën maakt, maar dit doorgaans overlaat aan de systeembeheerder van het onderzochte bedrijf, waarbij weinig tot geen tijd wordt gegund aan het bedrijf om een en ander goed voor te bereiden. Er is twijfel over de geschiktheid van de systeembeheerder om te bepalen welke informatie voor het onderzoek van belang is. Allereerst mist zo iemand vaak het overzicht, zeker in grote organisaties, en daardoor is de kans aanwezig dat vitale (en ontlastende) informatie over het hoofd wordt gezien. Bovendien ontbreekt ervaring met het documenteren van zijn of haar acties. Er valt dus nog veel te verbeteren aan de digitale werkwijze, en ook bedrijven zelf doen er verstandig aan om goed in kaart te brengen welke bedrijfsinformatie zich waar bevindt en hoe die efficiënt verzameld kan worden.

2.3 Economische criminaliteit

Hiervoor heb ik het toenemende belang geschetst van elektronische informatie in een bedrijfsomgeving. Dat belang is onderstreept door nieuwe wet- en regelgeving die is geïntroduceerd naar aanleiding van boekhoudfraudes zoals die van Enron en Ahold. Het belang van de digitale waarheid wordt nog duidelijker als we niet alleen naar boekhoudfraudes kijken, maar ook naar andere vormen van economische criminaliteit. Zo werden we in Europa een aantal jaren geleden opgeschrikt door smeergeldpraktijken bij Daimler en Siemens in Duitsland. Omkoping is een strafbaar feit en vooral in de VS wordt in het kader van de Foreign Corrupt Practices Act (FCPA) streng toezicht gehouden op beursgenoteerde bedrijven die zaken doen buiten de VS.[4] Omkoping staat op de tweede plaats op de lijst van meest voorkomende economische delicten in de Economic Crime Survey die iedere twee jaar door Pricewaterhouse-

Coopers wordt uitgebracht. In deze survey wordt een analyse uitgevoerd op de aard van economische criminaliteit in 54 landen.

Economic Crime Survey 2009

In 2009 heeft PricewaterhouseCoopers (PwC) de vijfde editie van de Global Economic Crime Survey (hierna: GECS) gepubliceerd.[5] PwC laat elke twee jaar een wereldwijde enquête uitvoeren om meer inzicht te krijgen in de oorzaken van fraude en de consequenties daarvan voor organisaties. Daardoor kunnen organisaties van de resultaten leren en deze bijvoorbeeld implementeren in hun preventie. Wereldwijd hebben in 2009 meer dan 3.000 respondenten uit 54 landen de daartoe uitgezette vragenlijsten ingevuld en van commentaar voorzien. De resultaten zijn samengevat in de GECS 2009. Waar mogelijk zijn de Nederlandse resultaten met de West-Europese en wereldwijde resultaten vergeleken.

Van de Nederlandse organisaties geeft 15% aan in het afgelopen jaar door fraude te zijn getroffen, bijna een op de zes. Wereldwijd is dit 30% en in West-Europa 20%. In voorgaande jaren in Nederland was dat nog 35%. Bijzonder verrassend is dat in Nederland maar liefst driekwart van de gevallen van fraude gepleegd is door iemand in de organisatie. Overigens ligt dit wereldwijd en in West-Europa rond de 50% en was het in de vorige Survey in Nederland 45%. Het uitbannen van economische criminaliteit is geen haalbare zaak, en daarom zullen onderzoek naar fraude en digitaal bewijs belangrijk blijven.

De belangrijkste economische delicten waar Nederlandse organisaties door getroffen worden, zijn boekhoudfraude en verduistering van geld en goederen. In de Nederlandse situatie worden andere economische delicten, in vergelijking met West-Europese en wereldwijde resultaten, veel minder vaak gemeld. Een verklaring hiervoor zou kunnen zijn dat deze vormen van economische criminaliteit relatief eenvoudig te ontdekken zijn. Andere vormen zijn veel lastiger te ontdekken en vereisen geavanceerde detectiemaatregelen in het kader van een adequaat stelsel van checks and balances. Opvallend is verder de relatief hoge score van de delictvorm 'illegaal handelen met voorkennis' in de Nederlandse situatie versus de rest van de wereld.

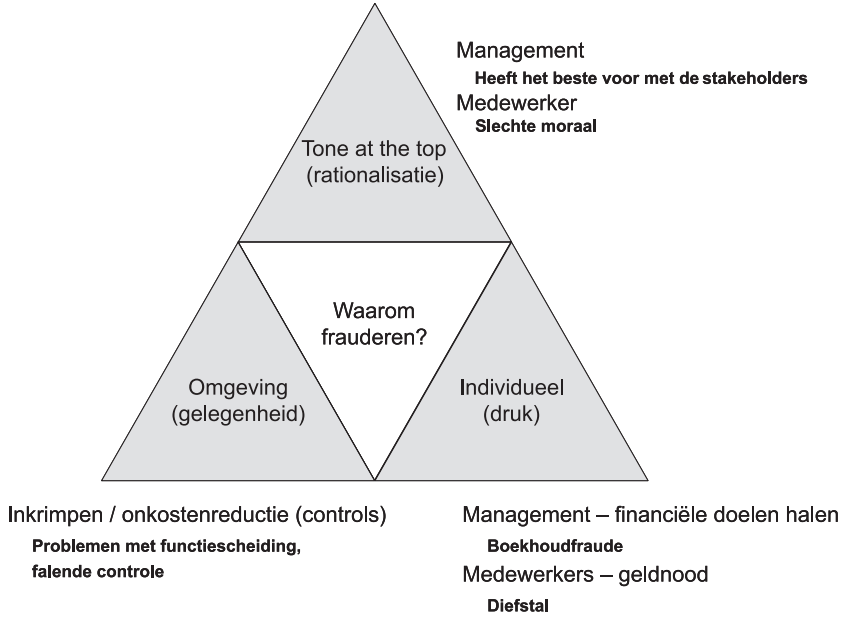
Wereldwijd is er een grote spreiding in de omvang van de geconstateerde schade als gevolg van een economisch delict. Bijna één op de tien organisaties rapporteert een schade die groter is dan 3,5 miljoen euro. Wereldwijd ligt in bijna de helft van de gevallen dit bedrag onder de 70.000 euro. Daar-

entegen wordt in Nederland in negen van de tien gevallen aangegeven dat de schade onder dit laatstgenoemde bedrag is gebleven. Slechts één op de tien rapporteert een aanzienlijk hogere schade. Een mogelijke oorzaak zou kunnen zijn dat de omvang van de responderende organisaties gemiddeld gezien in Nederland wellicht kleiner is in vergelijking tot West-Europa en wereldwijd.

Op de lijst met meest voorkomende vormen van economische criminaliteit in 2009 staat wereldwijd omkoping op de tweede plaats en in Nederland op de derde plaats. Op nummer één staat diefstal van geld of bedrijfsgoederen, zowel wereldwijd als in Nederland. Bedrijven komen liever niet in de publiciteit als zij het slachtoffer zijn van diefstal, vooral niet als het gaat om diefstal door eigen medewerkers. Toch zijn er talloze voorbeelden in de media te vinden van grootschalige oplichting. Het meest spectaculaire recente voorbeeld hiervan is de Madoff-fraude. De miljardenzwendel van Madoff werd in december 2008 ontdekt door de beurstoezichthouder in de VS, de U.S. Securities and Exchange Commission (SEC). Madoff beloofde beleggers zeer hoge rendementen en betaalde deze in eerste instantie met de inleg van nieuwe klanten. De SEC had overigens niet goed opgelet, want Madoff zou al sinds de jaren '70 op deze manier frauduleuze winsten maken.

Een interessant gegeven is dat vooral in tijden van economische crisis grootschalige fraude moeilijk is vol te houden. Naarmate de (financiële) markten krapper worden, worden tekorten sneller zichtbaar en zijn aandeelhouders en toezichthouders blijkbaar waakzamer. Een economische crisis geeft op zich ook aanleiding tot een toename van fraude. Dit kan verklaard worden aan de hand van de zogenaamde fraudedriehoek, die stelt dat de kans op fraude samenhangt met drie verschillende omstandigheden: gelegenheid of het gebrek aan controle, het voor zichzelf kunnen verantwoorden en de druk om fraude te plegen. Door de samenkomst van zowel financiële crisis als recessie ontstond de afgelopen jaren een 'Perfect Storm', waardoor omstandigheden op alle fronten verergerden. Mensen staan onder druk om bijvoorbeeld de reputatie van zichzelf of van het bedrijf te redden, of misschien wel omdat ze het geld van de bonus die ze niet krijgen al uitgegeven hebben. Tegelijkertijd zoeken bedrijven naar manieren om kosten te reduceren. Vooral als dit in korte tijd gebeurt, kunnen er onverwacht gaten in de controlemaatregelen vallen, waardoor de functiescheiding wegvalt die cruciaal is voor de interne controle. Ten slotte zal men in slechte tijden sneller geneigd zijn om frauduleuze handelingen te rationaliseren. Iemand die hard gewerkt heeft en onverwachts zijn bonus niet meer

krijgt, zal het misschien makkelijker kunnen rechtvaardigen om met een onkostendeclaratie te knoeien. Of bedrijven in moeilijke markten zullen wellicht toch overgaan tot het betalen van steekpenningen omdat de concurrenten dat ook doen. De fraudedriehoek wordt geïllustreerd in figuur 2.



Figuur 2: De fraudedriehoek in tijden van economische crisis

Nederland kent zo zijn eigen grote fraudes. In november 2007 werden we opgeschrikt door artikelen met krantenkoppen als 'Actie tegen vastgoedfraude', waarin stond: 'Met meer dan 500 medewerkers van de FIOD-ECD en 31 officieren van justitie heeft het Functioneel Parket van het Openbaar Ministerie (OM) gisteren een onderzoek gestart naar corruptie en omkoping in de vastgoedbeleggingssector'. Grote bedrijven als Fortis, Philips en Rabo Bouwfonds worden genoemd als slachtoffer (Van der Boon, 2007).

Een aantal van deze bedrijven heeft ook een intern onderzoek ingesteld om zelf na te gaan wat er precies aan de hand is. Het gaat daarbij om projecten en transacties die al vele jaren geleden hebben plaatsgevonden en waarvan de betrokken medewerkers vaak al niet meer in dienst zijn of binnen de organisatie van functie zijn veranderd. Het is niet vreemd dat een bedrijf in een periode van tien jaar al tweemaal van IT-infrastructuur is gewijzigd. Als in die periode bovendien overnames hebben plaatsgevonden is de kans groot dat er oude

systemen zijn geweest, waarvan de inhoud slechts gedeeltelijk of zelfs helemaal niet is overgenomen in de primaire bedrijfssystemen.

Het gaat niet eens zozeer om harde bewijzen, als wel om sporen die helpen de gang van zaken van jaren geleden in kaart te brengen. Veel van die sporen zijn te vinden in digitale informatie. Dit bleek onder andere uit een presentatie door de General Counsel van Siemens op de Corporate Accountability-conferentie die recent in Amsterdam werd georganiseerd.[6] Siemens bleek de afgelopen tien jaar maar liefst 1,3 miljard euro smeergeld te hebben betaald om internationale contracten binnen te halen. Het concern heeft hiervoor bij de Amerikaanse en Duitse autoriteiten een zware boete moeten betalen. Net twee dagen voor de conferentie had het bedrijf na vele mislukte pogingen eindelijk een schikking weten te treffen met zes ex-bestuurders die ieder vele miljoenen gaan betalen. Uit de presentatie bleek dat in het kader van het onderzoek naar de omkopingspraktijken in totaal 5.000 overeenkomsten, 40 miljoen bankafschriften, 100 miljoen documenten en 122 miljoen transacties in het boekhoudsysteem onderzocht zijn. Overigens is Siemens niet het enige bedrijf dat steekpenningen betaalde om contracten in de wacht te slepen. Het probleem speelt bij meerdere bedrijven in verschillende landen.

E-mail speelt een belangrijke rol bij het zoeken naar de digitale waarheid. Volgens het boek *De Vastgoedfraude* (Van der Boon en Van der Maarel, 2009) heeft de FIOD-ECD in de zaak die onder dezelfde naam bekend staat op 13 november 2007 elf terabyte aan digitale informatie verzameld. De auteurs van dit boek vermelden nog meer bijzonderheden, waaruit blijkt dat digitale informatie een belangrijke rol heeft gespeeld in het onderzoek. Met een speciaal programma 'Sherlock' doorzocht de FIOD-ECD deze informatieberg. Uit oude e-mail kon onder andere worden opgemaakt dat een verdachte, nadat hij vertrokken was bij het bedrijf waar hij werkte, toch nog projectinhoudelijke documenten kreeg doorgestuurd, en dat daarbij een 'zekere gedwongenheid' aan de orde was (p. 84). In het interne onderzoek bleken onderzoekers in staat om aan de hand van elektronische agenda's van anderen de agenda van een verdachte te reconstrueren, zodat meer inzicht werd verkregen in de samenwerkingsverbanden (p. 85). Een handgeschreven notitie leek een belangrijke aanwijzing te bevatten, maar was ondertekend met een onbekende afkorting. De verdachte, wiens naam wel overeenkomsten vertoont met de afkorting, ontkende de schrijver te zijn. Toen later van deze verdachte een e-mail gevonden werd die met dezelfde afkorting was ondertekend, leek het net zich langzaam te sluiten (p. 188). Het bewijs dat gevonden werd in digitale sporen stapelde zich verder op: Powerpointpresentaties met winstdelingen (p. 257), onderliggende overeenkomsten (p. 278) en zelfs hele spreadsheets met schaduwboekhoudingen (p. 259). Tegelijkertijd blijkt uit het boek dat de digitale informatie in dit onderzoek zeker niet doorslaggevend is, maar gecombineerd

wordt met andere onderzoekstechnieken. Soms kunnen e-mails wel van doorslaggevend belang zijn.

'Smoking gun' e-mails

In de *Financial Times* van 7 september 2005 stond een artikel getiteld 'Anything you e-mail may be used in evidence'. Aanleiding was de veroordeling van de Amerikaanse zakenbank Morgan Stanley door een rechtbank in Florida tot het betalen van een schadevergoeding en een boete van in totaal 1,45 miljard dollar aan een Amerikaanse investeerder. Het probleem was dat de bank niet in staat bleek om oude back-ups te doorzoeken en daardoor informatie onvolledig of niet op tijd kon produceren. Aan het einde van het artikel worden een aantal voorbeelden van zogenaamde 'smoking gun' e-mails gegeven, die van cruciaal belang zijn geweest in bekende schandalen:

- Een e-mail van een topmanager bij Shell, waarin hij aangaf 'sick and tired about lying' te zijn inzake de overgewaardeerde olie- en gasreserves. Deze e-mail kwam aan het licht in een intern onderzoek. Het schandaal zorgde ervoor dat de beurswaarde van Shell met miljarden dollars daalde en dat het bedrijf, zowel in de VS als in Europa, flinke boetes kreeg.
- Een technologieanalist van Credit Suisse First Boston is veroordeeld op grond van één e-mail aan zijn collega's, waarin hij hen vroeg om hun bestanden 'op te ruimen'.
- Een aandelenanalist van Merrill Lynch kreeg een boete van vier miljoen dollar en zijn werkgever een boete van honderd miljoen dollar nadat was gebleken dat hij via e-mail collega's had aangeraden om aandelen te kopen in bedrijven waar de bank voor werkte.

In het Enron onderzoek zijn soortgelijke e-mails ook naar voren gekomen, bijvoorbeeld:

- De CEO van Enron stuurde in augustus 2001 een e-mail naar medewerkers met de boodschap dat hij de vooruitzichten van Enron er rooskleurig vond uitzien. En dat terwijl hij kort daarvoor van een financiële medewerker een brief had ontvangen, waarin deze had aangegeven zich juist veel zorgen te maken in verband met mogelijke boekhoudschandalen.

Tot besluit nog een recent voorbeeld van een e-mail die een belangrijke rol speelde in een onderzoek van de Europese Commissie:

– In september 2009 werd, in het kader van een mededingingsonderzoek door de EU, e-mailverkeer openbaar tussen Intel en computerfabrikanten. Uit een e-mail van juli 2002 bleek dat ten gevolge van afspraken met Intel, HP niet meer dan vijf procent van zijn PC's met AMD-processors kon uitrusten.

Naast e-mail is ook de financiële administratie van grote waarde bij het in kaart brengen van diefstal. Net als bij onderzoeken naar corruptie staat de analyse van betalingen centraal. Wie zijn de leveranciers, hoeveel hebben zij ontvangen en is er ook daadwerkelijk iets geleverd? In veel gevallen is de aanleiding van het onderzoek één specifieke betaling waarbij sprake is van fraude. De vraag of er sprake is van andere soortgelijke frauduleuze betalingen ligt voor de hand. Het bedrijf wil natuurlijk weten hoe groot de fraude is. Het onderzoek spitst zich dan in veel gevallen toe op de koppeling van verschillende systemen. Bijvoorbeeld het identificeren van andere verdachte transacties in de financiële administratie en het vervolgens opzoeken van de bijbehorende facturen om te controleren of de omschrijving wel klopt, of om te kijken door wie de factuur geautoriseerd is. Naarmate de onderzoekers meer inzicht krijgen in de werkwijze van de fraudeur, zijn ze beter in staat om zoekvragen te formuleren en meer verdachte betalingen, facturen of leveranciers in kaart te brengen. Het identificeren van verdachte zaken met behulp van een handmatig ontdekt patroon is in eerste instantie vooral een geautomatiseerd proces. Dat proces vergt een speciaal digitaal onderzoek, omdat de standaardrapportages in de financiële administratie tekortschieten.

3. E-Discovery perspectieven

In het voorafgaande heb ik de ontwikkelingen geschetst in het onderzoek naar digitale informatie, en met voorbeelden toegelicht waarom het belangrijk is om de digitale waarheid te kennen. Niet alleen is de digitale waarheid belangrijk, bedrijven worden ook in toenemende mate verplicht om elektronische informatie in de vorm van records te managen onder druk van toenemende wet- en regelgeving en strenger wordende toezichthouders, zowel in nationaal als internationaal verband. De vraag is nu: hoe leren we de digitale waarheid kennen? Gegeven de enorme hoeveelheid en complexiteit van elektronische infor-

matie waar bedrijven tegenwoordig mee werken, lijkt het vinden van sporen in de enorme berg aan elektronische informatie veel op het zoeken naar een speld in een hooiberg.

Eigenlijk is het nog erger. Juist bij fraudeonderzoeken weten onderzoekers vaak niet eens precies waarnaar ze op zoek zijn. In rechtszaken in de VS wordt daarom gesproken van Legal Discovery. Als het gaat om het zoeken en ontdekken van sporen in elektronisch opgeslagen informatie (Electronic Stored Information, of in het kort ESI), dan wordt gesproken van Electronic Discovery, ook wel afgekort tot E-Discovery. Het werkterrein van E-Discovery bestaat uit een verzameling methoden en gereedschappen om digitale informatie te verwerken en te analyseren in de zoektocht naar de digitale werkelijkheid. E-Discovery kan gezien worden als een toegepaste multidisciplinaire wetenschap waarin technieken uit disciplines zoals informatica, recht, forensisch (computer)onderzoek, bedrijfskunde, forensische accountancy en informatiebeheer samenkomen.

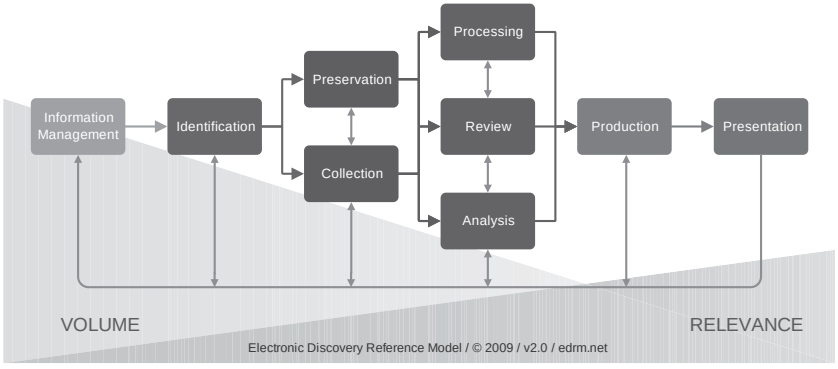
Het doel van E-Discovery is tweeledig: 1) elektronische data veiligstellen die mogelijk van belang zijn in een onderzoek, en 2) het in die data ontdekken van gegevens die van belang zijn voor het onderzoek, dan wel het aantonen dat bepaalde informatie niet aanwezig is. Nu zal ik vanuit verschillende perspectieven een indruk geven wat E-Discovery in de praktijk betekent, en welke methoden en technieken er worden gebruikt om digitale gegevens te identificeren en te kopiëren om ze vervolgens zodanig te verwerken dat ze gebruikt kunnen worden in bijvoorbeeld een onderzoek naar fraude. Daarna zal ik omschrijven op welke manier het lectoraat kan bijdragen aan de ontwikkeling van E-Discovery.

3.1 E-Discovery vanuit het EDRM-perspectief

E-Discovery kan gezien worden als een informatieverwerkend proces. Het Electronic Discovery Reference Model (EDRM) beschrijft de verschillende onderdelen in dat proces en hun onderlinge samenhang. Figuur 3 bevat een schema van het EDRM.

Het EDRM is in 2005 bedacht door George Socha en Tom Gelbmann in een poging om een gemeenschappelijk kader te creëren voor E-Discovery professionals met verschillende achtergronden. Hun doel was om deze specialisten bij elkaar te brengen om samen een aantal lastige E-Discovery problemen op te kunnen lossen. Het aantal deelprojecten is gestaag uitgebreid en heeft onder andere geleid tot de publicatie van een EDRM XML-standaard en sets met testdata. Het EDRM zelf blijft echter het meest bekende product van deze groep en is goed bruikbaar om de verschillende onderdelen van E-Discovery uit te leggen:

1. Informatiemanagement: Het managen van informatie vanaf het moment van aanmaken, gebruiken, tot en met het moment dat informatie die niet meer in gebruik is gearchiveerd dan wel vernietigd moet worden. Dit is een algemeen proces binnen de organisatie, waarvan verondersteld wordt dat het op orde is. Is dit proces niet op orde, dan zal dit onvermijdelijk nadelige gevolgen hebben voor de vervolgstappen in het proces.



Figuur 3: Electronic Discovery Reference Model (www.edrm.net)

2. Identification: Identificatie is het eerste proces waarin gereageerd wordt op een E-Discovery verzoek. In dit proces moeten potentiële informatiebronnen gelokaliseerd worden en moet de scope van het onderzoek vastgesteld worden. Met 'scope' wordt hier bedoeld de vraag om welke informatie het gaat (projecten, medewerkers, afdelingen enzovoorts) en om welke periode. Dit onderdeel is een belangrijke stap, omdat hiermee direct de omvang van het vervolgonderzoek bepaald wordt.
3. Preservation: Het veiligstellen van informatie, zodanig dat deze niet meer gewijzigd of vernietigd kan worden. Dit kan betekenen dat informatie gekopieerd wordt, maar het kan ook betekenen dat andere maatregelen genomen worden om dit te bewerkstelligen. Bijvoorbeeld door back-up tapes zo te markeren dat ze niet meer gerecycled worden in een back-up schema.
4. Collection: In dit proces wordt informatie daadwerkelijk verzameld (meestal gekopieerd) om verder gebruikt te worden in het E-Discovery proces. In veel gevallen worden preservation en collection gelijktijdig uitgevoerd. Bijvoorbeeld door gegevens te kopiëren en een secure hash code

te berekenen waarmee later de integriteit van gegevens aangetoond kan worden.

5. Processing: De verzamelde gegevens worden verwerkt met als doel het volume te verkleinen en gegevens in een leesbare vorm om te zetten. Bij verwerking moet bijvoorbeeld gedacht worden aan:
   - verwijderen van dubbele exemplaren;
   - doorzoekbaar maken en filteren van bestanden op grond van vooraf vastgestelde zoektermen;
   - aanbrengen van meer structuur door de extractie van meta-informatie (bijvoorbeeld e-mailheadergegevens, MsOffice document properties, bestandspad van herkomst);
   - extractie van bestanden uit archieven en bijlagen uit e-mail.
6. Review: Uiteindelijk zal de informatie die na verwerking overblijft door onderzoekers beoordeeld moeten worden. Verwerkte gegevens zijn weliswaar leesbaar, maar alleen met een passende review oplossing kan een team reviewers effectief gezamenlijk gegevens bekijken.
7. Analysis: Een grondige analyse is nodig om patronen en verbanden te vinden die belangrijk zijn voor het onderzoek. Een review is meestal oppervlakkiger en daarmee geschikter om een grotere hoeveelheid informatie relatief snel te beoordelen. De resultaten van de review worden in veel gevallen gedetailleerder onderzocht. In sommige gevallen is er geen tijd of capaciteit voor een review en zullen onderzoekers bij hun analyse in de verwerkte informatie zoeken en die beoordelen.
8. Production: Productie houdt in het opleveren van elektronische gegevens aan derden, in een afgesproken formaat via een afgesproken protocol. Het betreft hierbij alleen de gegevens die relevant zijn bevonden als een resultaat van de verwerking, review en/of analyse.
9. Presentation: Bij de presentatie gaat het erom de gegevens te presenteren in (bijna) originele vorm, om zodoende betrokken partijen te informeren en een reactie te krijgen. Dit kan van toepassing zijn in een rechtszaak, maar ook bij een interview met een betrokkene.

3.2 E-Discovery vanuit een strategisch perspectief

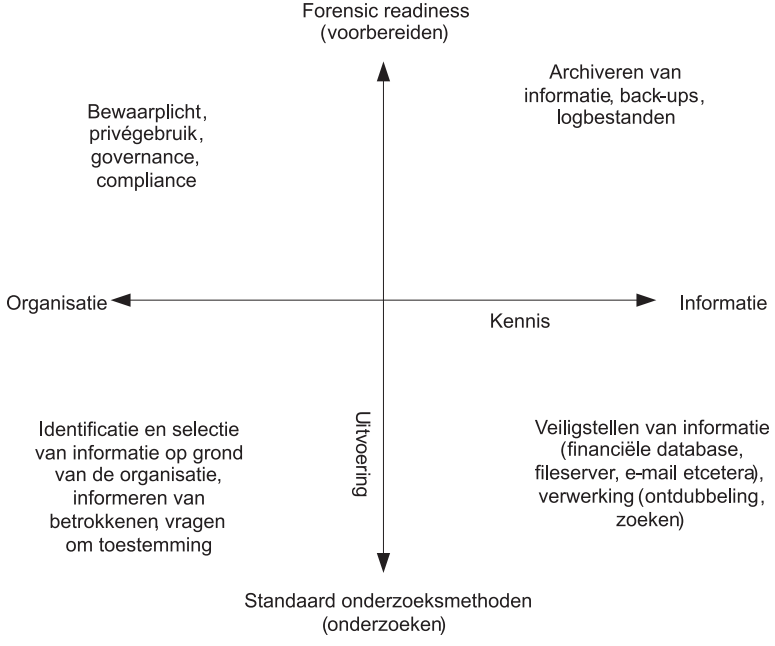
Hiervoor heb ik aan de hand van het EDRM uitgelegd uit welke stappen E-Discovery bestaat. Maar ik wil E-Discovery ook in een strategisch perspectief plaatsen. Bij de bepaling van de E-Discovery strategie zijn zowel kennis als uitvoering van belang.

Kennis op het gebied van E-Discovery bevindt zich in twee uitersten. Aan de ene kant bevindt zich de kennis over de organisatie en de bedrijfsprocessen. Deze kennis is onmisbaar om te kunnen bepalen welke gegevens belangrijk

zijn voor het onderzoek. Aan de andere kant bevindt zich de kennis die nodig is om met de verschillende soorten informatie om te gaan in het kader van E-Discovery.

Ten aanzien van de uitvoering onderscheiden we aan de ene kant het voorbereid zijn op E-Discovery – forensic readiness – en aan de andere kant het daadwerkelijk uitvoeren van E-Discovery, dat in de praktijk volgens standaardonderzoeksmethoden verloopt.

Figuur 4 illustreert dit perspectief van kennis en uitvoering van E-Discovery en brengt deze ook met elkaar in verband. Met kennis van de organisatie en processen kan gekeken worden naar zowel de voorbereiding op een forensisch onderzoek (forensic readiness) als naar het onderzoek in uitvoering. Het gaat daarbij vooral om informatiemanagement en identificatie, beide onderdelen van het EDRM. Bij het kiezen van een E-Discovery strategie moet een organisatie zich afvragen in welke mate ze voorbereid wil zijn (preventief), en in staat is om projecten uit te voeren als er daadwerkelijk informatie verzameld moet worden.



Figuur 4: E-Discovery strategie

In zowel de voorbereiding als de uitvoering speelt kennis over organisatie en informatie een centrale rol. De rechterkant van figuur 4 richt zich op kennis over informatie en de applicaties waarmee die informatie wordt beheerd. Bij de uitvoering van het onderzoek zijn kennis en methoden nodig om informatie op forensische manier veilig te stellen en te verwerken. Met betrekking tot forensic readiness wordt kennis verwacht van bijvoorbeeld de applicaties en hoe die het beste ingericht kunnen worden om in een onderzoek zinvolle informatie snel en efficiënt veilig te kunnen stellen. Het gebied rechtsonder is het meest verwant met de inhoud van de elektronische informatie.

De linkerkant van figuur 4 is gericht op de organisatie: hoe zijn de bedrijfsprocessen georganiseerd en welke informatiestromen hangen daarmee samen? Ook op organisatorisch gebied kan een bedrijf vooraf strategische voorbereidingen treffen. Maar uiteindelijk zal bij de feitelijke uitvoering van het E-Discovery onderzoek ook rekening gehouden moeten worden met de structuur van de organisatie in zowel het heden als het verleden.

3.3 E-Discovery vanuit een informatie-technisch perspectief

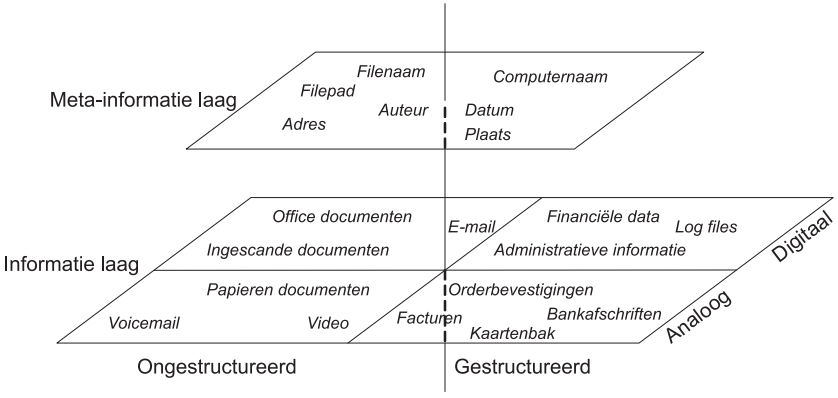
In het EDRM speelt, na het identificeren en veiligstellen van informatie, de automatische verwerking van informatie een belangrijke rol. Het gaat daarbij vooral om de eliminatie van niet-relevante informatie. Hoe meer onnodige informatie op een automatische manier verwijderd kan worden, des te minder informatie blijft er over om handmatig geanalyseerd te worden.

Een overzicht van de soorten informatie geeft inzicht in dit domein. Daarbij maken we onderscheid in twee eigenschappen van informatie, namelijk gestructureerde versus ongestructureerde informatie en analoge versus digitale informatie. Dit levert een kwadrant op, weergegeven in de onderste laag in figuur 5.

Het E-Discovery informatiekwadrant kwalificeert in eerste instantie de inhoud (content) van informatie aan de hand van de vorm van de ruwe data. Naast deze data is ook meta-informatie beschikbaar. Meta-informatie stelt de context voor van informatie en is in figuur 5 weergegeven als een laag boven de informatielaag – met dien verstande dat meta-informatie per definitie gestructureerd en tegenwoordig ook bijna altijd digitaal voorhanden is. Meta-informatie kan enerzijds al aanwezig zijn door de natuurlijke information lifecycle van informatie binnen de organisatie, maar kan ook automatisch of met de hand gecreëerd worden als onderdeel van E-Discovery.

Dit betekent dat informatieverwerking in E-Discovery moet kunnen omgaan met bestaande content en gerelateerde meta-informatie. Daarbij is als onderdeel van het verwerkingsproces het op gestructureerde wijze beschikbaar houden van bestaande en de creatie van nieuwe meta-informatie van strate-

gisch belang. Het creëren (vaak extraheren) van meta-informatie biedt aanknopingspunten om content te filteren tijdens de verwerking. Bij bestaande meta-informatie kan het gaan om de herkomst van gegevens tijdens het verzamelen, en bij nieuwe meta-informatie om bijvoorbeeld e-mailheaders, bestandspaden, auteur, de relatie tussen e-mail en bijlage, enzovoorts. Het is zaak om bestaande meta-informatie en nieuwe meta-informatie samen te voegen, zodat er een compleet overzicht is.



Figuur 5: Informatiekwadrant met meta-informatie

Uiteindelijk speelt het type informatie een grote rol bij de analyse van informatie. Een bestand met semi-gestructureerde informatie kan door middel van een relatief eenvoudige conversie gestructureerd worden (als werkblad in een spreadsheet of als tabel in een database). Analyse van gestructureerde informatie vereist speciale kennis van de database en vaardigheden om met databases met gestructureerde informatie om te gaan (bijvoorbeeld het formuleren van SQL database queries). De analyse van ongestructureerde informatie is lastig te automatiseren. In veel gevallen zit er weinig anders op dan de verwerkte documenten (e-mails enzovoorts) door te lezen. Er bestaan echter veelbelovende text mining en data mining technieken die met de huidige snelle computers en grote geheugens heel goed structuur kunnen vinden in ongestructureerde informatie, of waarmee nieuwe patronen en verbanden ontdekt kunnen worden in grote hoeveelheden onoverzichtelijk gestructureerde informatie. Voorbeelden van dergelijke toepassingen zijn het automatisch maken van samenvattingen, het ontdekken van (onbekende) namen van personen, plaatsen en relaties in documenten, het identificeren van documenten die maar weinig van

elkaar verschillen en het visualiseren van patronen in grote hoeveelheden financiële transacties.

3.4 E-Discovery vanuit een juridisch perspectief

Door de letterlijk onbegrensde mogelijkheden van internet en door de globalisatie van economische activiteit (en criminaliteit), vereist E-Discovery een multinationale aanpak. Door de grote verscheidenheid in nationale wetgeving is cross-border E-Discovery een thema dat op dit moment veel aandacht krijgt. Die aandacht voor internationale aspecten is niet nieuw. De eerder geschetste automatisering van de georganiseerde misdaad in de jaren '90 zorgde al voor de noodzaak tot internationale samenwerking. Dit heeft onder andere geleid tot de oprichting van de International Organisation on Computer Evidence (IOCE). Op verzoek van de werkgroep voor high-tech crime van de G8 (het forum van acht vooraanstaande industriële staten) heeft de IOCE een aantal principes geformuleerd die betrekking hebben op de omgang met digitaal bewijs.

IOCE-principes voor de omgang met digitaal bewijsmateriaal

De International Organisation on Computer Evidence (http://www.ioce.org) werd opgericht in 1992 en speelt met name een rol in de internationale samenwerking tussen nationale politieorganisaties. In 1997 organiseerde ik met mijn team van het Gerechtelijk Laboratorium de jaarlijkse IOCE-conferentie die toen in Den Haag werd gehouden. De conferentie was een groot succes en werd bezocht door 92 deelnemers uit 20 verschillende landen vanuit alle werelddelen. In 1998 wees de G8 high-tech crime subgroup de IOCE aan om internationale basisprincipes op te stellen voor procedures om digitaal bewijs te verzamelen en te verwerken. Aan deze principes wordt nog vaak gerefereerd in de vele verschillende regionale handleidingen die betrekking hebben op het verwerken van digitaal bewijs.

Daarop werden in 2000 door de IOCE de volgende principes geïntroduceerd:

- Bij digitaal bewijs moeten alle algemene forensische principes en procedures toegepast worden.
- Bij het verzamelen van digitaal bewijs moeten voorzorgsmaatregelen genomen worden, zodat het bewijs niet gewijzigd wordt.
- Indien een persoon toegang tot het originele bewijsmateriaal krijgt, moet deze persoon getraind zijn voor dat doel.

– Alle activiteiten met betrekking tot inbeslagname, toegang, opslag of transport van digitaal bewijs moeten volledig gedocumenteerd worden en beschikbaar zijn voor inspectie.
– Een individu is verantwoordelijk voor alle acties die worden ondernomen met het digitale bewijs, zolang het in zijn of haar bezit is.
– Iedere organisatie die verantwoordelijk is voor verzameling, toegang, opslag of transport van digitaal bewijs wordt geacht zich aan bovenstaande principes te houden.

Deze principes zijn door de IOCE aan de G8 subgroup voor high-tech crime voorgelegd, die ze vervolgens heeft goedgekeurd. De principes zijn door verschillende landen overgenomen.

Gelijktijdig met de verspreiding van de G8-principes voor het omgaan met digitaal bewijs werd medio 2002 een werkgroep ingesteld door een groep juristen en advocaten, die zich georganiseerd hebben in The Sedona Conference.[7] Deze werkgroep ging zich bezighouden met het thema bewaren en produceren van elektronische documenten. De richtlijnen die door de werkgroep zijn gepubliceerd hebben een grote invloed gehad op de totstandkoming van de eerdergenoemde Federal Rules of Civil Procedure in de VS.

Principes en richtlijnen van The Sedona Conference

Begin 2003, een half jaar na de eerste bijeenkomst van werkgroep WG1, worden de *Sedona Principles* gepubliceerd (The Sedona Conference, 2003). Deze 14 principes tonen dan al veel facetten van onderdelen die in 2006 in de nieuwe Federal Rules of Civil Procedure worden opgenomen. Na het verschijnen van de aangepaste FRCP in december 2006, heeft Sedona WG1 een tweede editie uitgebracht (The Sedona Conference, 2007a).

Eind 2007 heeft WG1 the *Sedona Guidelines* gepubliceerd (The Sedona Conference, 2007b). Deze richtlijnen zijn vooral bedoeld om een kader te scheppen voor organisaties om a) hun eigen voorschriften, werkwijzen en procedures te evalueren, en b) om te komen tot een best practice voor het managen van informatie. Voorts heeft WG1 in 2007 verschillende documenten geschreven die rechtstreeks betrekking hebben op E-Discovery,

waaronder een begrippenlijst en een uitgebreid document met tips op welke manier het beste leveranciers van E-Discovery diensten en software geselecteerd kunnen worden.

De meest recente publicatie van Sedona WG1 dateert uit mei 2009 (The Sedona Conference, 2009). Deze publicatie is gericht op het verhogen van de kwaliteit van een E-Discovery proces. Naast diverse principes die worden beschreven, ligt de nadruk vooral op goed projectmanagement om de kwaliteit van een E-Discovery proces te waarborgen.

Eind 2003 realiseerden deelnemers van The Sedona Conference zich dat E-Discovery een zeer belangrijke internationale dimensie heeft. Via een nieuwe Sedona werkgroep werd een internationale dialoog gestart over management en discovery van elektronische data. Dit is de Sedona werkgroep voor 'International Electronic Information Management, Discovery and Disclosure', afgekort Sedona WG6. In 2008 heeft Sedona WG6 een gids uitgebracht met praktische tips over hoe te navigeren tussen de tegenstrijdige belangen van internationale data privacy en E-Discovery (The Sedona Conference, 2008).

In veel opzichten botsen de Federal Rules of Civil Procedure in de VS met de privacywetgeving in andere delen van de wereld en vooral met die van continentaal West-Europa. Het is niet ongewoon dat een Nederlands bedrijf met een vestiging in de VS wordt gevraagd om in het kader van pre-trial discovery e-mails ter beschikking te stellen aan de advocaat van de tegenpartij in een juridisch conflict, iets wat indruist tegen onze nationale privacywetgeving. In het verleden werd bij dit soort internationale rechtshulpverzoeken een beroep gedaan op het Verdrag van Den Haag uit 1970 inzake de verkrijging van bewijs in het buitenland in burgerlijke en handelszaken. In dit verdrag is echter geen rekening gehouden met de manier waarop wij tegenwoordig met elektronische informatie omgaan, namelijk dat bedrijfsmatige en privécorrespondentie met elkaar vermengd zijn, en ook dat bedrijfsinformatie die automatisch is verwerkt vaak eenvoudig tot een persoon is te herleiden.

Onze privacy komt vooral in het geding door de verschillen tussen de Engels/Amerikaanse juryrechtspraak (common law) en onze rechtspraak waarbij de rechter een belangrijke rol speelt (civil law). Bij juryrechtspraak bestaat de eerdergenoemde pre-trial discovery. In die fase (voordat de zaak voor de rechter komt) worden partijen geacht potentieel bewijsmateriaal (bijvoorbeeld e-mails) beschikbaar te stellen. Deze verzoeken kunnen vrij breed geformuleerd worden, terwijl in sommige Europese landen, zoals Frankrijk, een partij alleen

via de rechter om inzage kan vragen als exact aangegeven kan worden om welk document het gaat, wat juist met de enorme hoeveelheden informatie die bij E-Discovery aan de orde zijn geen haalbare zaak is. Deze verschillen hebben tot een patstelling geleid waarbij landen zogenaamde 'blocking statutes' hebben aangenomen die het uitleveren van persoonsgerelateerde informatie aan het buitenland strafbaar stellen.

Huidige technieken voor informatieverwerking lijken een oplossing te bieden voor dit voortslepende conflict. In essentie komt het erop neer dat partijen objectieve zoekcriteria kunnen afspreken om de beschikbare elektronische informatie te filteren. Door de groei van de hoeveelheid informatie zijn traditionele zoektechnieken echter niet toereikend. Andere, meer geavanceerde technieken zijn nodig om op een objectieve manier de hoeveelheid informatie effectief te kunnen beperken zonder dat de privacy van betrokkenen wordt geschaad.

In een speciaal daarvoor opgezet project heeft WG1 van The Sedona Conference de mogelijkheden van state of the art search & retrieval technology (hierna vertaald als 'zoektechnologie') onderzocht in de context van een civiel proces en het naleven van regelgeving in het digitale tijdperk (The Sedona Conference, 2007c). Het doel daarvan is om alle spelers in het rechtsproces een richtlijn te verschaffen op het gebied van E-Discovery zoektechnologie. Dit belang groeit vanwege de noodzaak om accuraat en efficiënt naar bewijs te zoeken in de explosief groeiende hoeveelheid digitale informatie die onderwerp kan worden van een civiel proces, of van een intern of extern onderzoek, bijvoorbeeld door een toezichthouder. Deze Sedona-publicatie biedt een interessant overzicht van bestaande zoektechnologieën en geeft praktische richtlijnen voor een objectieve evaluatie van deze technieken. Minstens zo interessant is de slotparagraaf waarin toekomstige ontwikkelingen geschetst worden, waarbij een brug geslagen wordt tussen ontwikkelingen in de artificiële intelligentie en het proces van legal discovery.

De meesten van ons zal het inmiddels duizelen van 'The Sedona Conference' principes, richtlijnen en aanbevelingen. Daarom wil ik tot slot nog een analogie beschrijven van een soortgelijke situatie waarin een door technologie veroorzaakt privacyprobleem uiteindelijk ook weer met technologie opgelost kan worden. Neem de uitvinding van de full-body scan die wordt ingezet bij de controle van vliegtuigpassagiers, en zeer recentelijk in de publiciteit is gekomen na de mislukte aanslag op een vlucht van Amsterdam naar Detroit. Deze scan werkt zo goed, dat er door de kleren heen gekeken wordt zonder schadelijke straling. In feite wordt een naaktfoto gemaakt, zodat bijzondere voorwerpen snel ontdekt kunnen worden. Dit is bijzonder effectief, maar passagiers zijn van mening dat hiermee een inbreuk gemaakt wordt op hun privacy. Onlangs is nieuwe software beschikbaar gekomen waarmee een computer de fo-

to's kan beoordelen, zodat het niet langer nodig is dat menselijke operators naar de beelden kijken. Hiermee lijkt het bezwaar ten aanzien van privacy opgelost te zijn. Een dergelijke oplossing is ook nodig voor E-Discovery.

4. De agenda van het Lectoraat E-Discovery

Tot nu toe heb ik het belang van de digitale waarheid geschetst en een indruk gegeven van de stand van zaken op het werkterrein van E-Discovery. In het resterende gedeelte van deze les wil ik ingaan op de bijdrage die het lectoraat kan leveren aan de verdere ontwikkeling van E-Discovery.

In de eerste helft van 2009 heeft het lectoraat geïnvesteerd in de oprichting van een Kenniskring die bestaat uit docenten van het Domein Media, Creatie en Informatie. De Kenniskring heeft een agenda opgesteld en is daarmee de tweede helft van het jaar aan de slag gegaan. Ik zal nu nader ingaan op deze agenda en de keuzes die gemaakt zijn op het gebied van onderwijs en onderzoek.

4.1 E-Discovery thema's

De verschillende perspectieven die hiervoor gepresenteerd zijn, laten zien dat het onderwerp E-Discovery multidisciplinair en zeer breed is. Om met de huidige Kenniskring succesvol onderzoek te doen is het noodzakelijk om accenten aan te brengen door in eerste instantie te kiezen voor de volgende drie E-Discovery thema's:

1. Digitale sporen in e-mail
2. Digitale sporen in data warehouses
3. Forensic readiness

Deze drie thema's bepalen het E-Discovery onderzoek en onderwijs van het lectoraat op de korte termijn. Waarom is juist voor deze drie thema's gekozen?

1. Digitale sporen in e-mail

E-mail is een van de meest aansprekende vormen van elektronische informatie, en kan van wezenlijk belang zijn bij de waarheidsvinding in een onderzoek. Bovendien is e-mail een toegankelijke vorm van informatie die zich goed leent voor onderzoek en experimenten. Tegelijkertijd is e-mail ook een lastige vorm van elektronische informatie, vanwege de informele en soms persoonlijke aard van de informatie en de slecht gestructureerde opslag. Dat maakt het effectief verzamelen en verwerken van e-mail tot een interessante technische uitdaging.

Technische uitdagingen bij het verzamelen van e-mail

E-mails kunnen helpen om gericht vragen voor te bereiden. Maar de praktijk is weerbarstig en het is niet eenvoudig om e-mails van betrokkenen, die mogelijk al jaren eerder het bedrijf hebben verlaten, volledig te verzamelen over een periode van tien jaar. Het verzamelen van deze informatie is een onderzoek op zich. Meestal gaan back-ups van file servers niet verder terug dan drie jaar en back-ups van e-mailservers gaan tegenwoordig niet verder terug dan twee maanden. Bij e-mail is het aan de gebruiker zelf om te bepalen welke informatie hij wel en niet wil bewaren. Als uit een interview blijkt dat de organisatie ergens rond de eeuwwisseling gemigreerd is van Exchange Server 5.5 naar Exchange Server 2000, dan is het bijzonder interessant als in een IT-ruimte een oude tape met opschrift Exchange 5.5 migratie uit het jaar 2000 gevonden wordt.

Hierdoor wordt in veel gevallen e-mail verzameld uit persoonlijke e-mailarchieven die medewerkers aanleggen op persoonlijke of gedeelde netwerkschijven. Zulke e-mailarchieven kunnen meestal wel verzameld worden, maar het is onduidelijk in hoeverre de informatie in die archieven compleet is. De beste strategie is om alle gevonden archieven samen te voegen, inclusief de archieven die gevonden zijn op back-ups. Liefst niet alleen van de betrokken personen, maar ook van hun collega's. Gebruikers kunnen immers wel e-mails in hun eigen mailbox wissen, maar niet de e-mails in andere mailboxen van de afzenders of van de geadresseerden. In de praktijk betekent dit wel dat er veel dubbele e-mails aanwezig zijn die het onderzoek vertragen. Hiervoor zijn echter doeltreffende ontdubbelingstechnieken waarmee dubbele e-mails verwijderd kunnen worden.

2. Digitale sporen in data warehouses

Voor data warehouses geldt eigenlijk, in tegenstelling tot e-mail, dat de informatieopslag juist heel goed georganiseerd is. Toch vormen ook digitale sporen in data warehouses een dankbaar onderwerp voor de Kenniskring, want bij een onderzoek naar economische fraude is inzicht in de financiële administratie onmisbaar, en op dit moment nog onderbelicht. Het is een technische uitdaging om elektronische gegevens in een data warehouse te verwerken, doordat ze alleen betekenis krijgen als ze in de context van de bedrijfsprocessen worden geanalyseerd. Dat vereist een bijzondere samenwerking tussen E-Dis-

covery specialisten en (inhoudelijke) onderzoekers, zoals forensische accountants, advocaten of inspecteurs van een toezichthouder.

Sporen zoeken in een data warehouse

Zoals de naam al doet vermoeden, herbergen data warehouses grote hoeveelheden data. Veel bedrijven hebben een enterprise resource planning (ERP) data warehouse. Dat is een systeem waarin bedrijfsinformatie zoals betalingen, voorraad, boekhouding enzovoorts wordt bijgehouden. Informatie in een data warehouse speelt een belangrijke rol bij het opsporen van fraude. Zo kan diefstal door fraude in de betalingenadministratie lange tijd verborgen blijven voor controlerende accountants. Bijvoorbeeld als medewerkers bankrekeningnummers tijdelijk kunnen wijzigen zonder dat dit in de administratie te zien is. Ook in een onderzoek naar integriteit wordt in het data warehouse gezocht naar, bijvoorbeeld, eenmalige leveranciers, provisies, nul-euro facturen en betalingen met ronde bedragen.

In tegenstelling tot file servers en e-mailservers, bevatten de data warehouses relatief kleine berichten met een vastgelegde structuur: database records. Deze records zijn verzameld in tabellen. Zulke tabellen hebben een onderlinge samenhang die in de meeste gevallen impliciet wordt bepaald door de geautomatiseerde systemen waarin de records verwerkt worden. Dat maakt het zoeken in een data warehouse bepaald niet eenvoudiger. Het probleem is namelijk dat de informatie die in een standaardoverzicht wordt verstrekt, veelal voor een forensisch onderzoek niet toereikend is. Dat betekent dat E-Discovery specialisten zelf de samenhang van verschillende tabellen moeten begrijpen om de informatie te achterhalen die voor het onderzoek nodig is.

Vanuit forensisch perspectief is voorzichtigheid geboden, want hoe weten de onderzoekers zeker dat er geen informatie is verloren gegaan of dat er geen informatie is gewijzigd? Daarom is het toetsen van de volledigheid en correctheid van de ruwe informatie die uit een data warehouse wordt verkregen een belangrijke (maar wel tijdrovende) stap. Bij een onderzoek naar malversaties in de boekhouding zullen E-Discovery specialisten de gekopieerde financiële informatie uit het grootboek altijd eerst op volledigheid controleren. Dat doen ze bijvoorbeeld door een herberekening te maken van een proefbalans en deze te vergelijken met de proefbalans die door het financiële systeem is geproduceerd.

3. Forensic readiness

Ten slotte is als derde thema forensic readiness gekozen, omdat hierdoor kennis en ervaring met E-Discovery preventief inzetbaar wordt gemaakt. Voor een hogeschool zal het in de praktijk moeilijk zijn om studenten en onderzoekers E-Discovery werkzaamheden te laten verrichten in daadwerkelijke fraudeonderzoeken. Door een methode te ontwikkelen waarmee in kaart gebracht kan worden wat, als het tot een onderzoek zou komen, de zwakke punten van een organisatie op het terrein van E-Discovery zijn, is het toch mogelijk bedrijven in de praktijk op het gebied van E-Discovery te adviseren.

In het navolgende werk ik het onderzoek en het onderwijs van het Lectoraat E-Discovery uit. Tot slot geef ik daarna aan hoe de Kenniskring buiten de Hogeschool zal samenwerken met andere partijen die betrokken zijn bij E-Discovery.

4.2 E-Discovery onderzoek

Aan de hand van de hiervoor geschetste thema's kan het onderzoek naar E-Discovery in een drietal kaders uitgewerkt worden:

a. Onderzoeksvaardigheden (forensisch)
b. Methoden en technieken (informatica, informatiemanagement)
c. Ethische en juridische aspecten (privacy, bewaarplicht)

In de tabel hieronder worden thema's en kaders in een matrix neergezet. In de cellen van de matrix staan de concrete onderwerpen die door de Kenniskring worden uitgewerkt.

Onderzoeksmatrix Kenniskring E-Discovery	1. E-mail discovery	2. Data warehouses	3. Forensic readiness
A. Onderzoeksvaardigheden	Rol van e-mail in een onderzoek. Inrichten en managen van het review proces.	Rol van data warehouses in het onderzoek.	Forensic readiness framework.

B. Methoden en technieken	Digitale wasstraten. Sporen van webmail. Visualisatie van communicatiepatronen.	Data acquisitie. SQL. Data mining. Visualisatie.	Meetbaar maken (auditplan). Sourcing aspecten. Serious game.
C. Ethische en juridische aspecten	Hoe omgaan met privé e-mails. Status van verwijderde en versleutelde gegevens.	Privacyaspecten bij koppelen gegevens financiële administratie met personeelsadministratie.	Afspraken maken over privégebruik e-mail. Bewaarplicht, vernietiging en digitaal archiveren.

Tabel 1: Onderzoeksmatrix Kenniskring E-Discovery

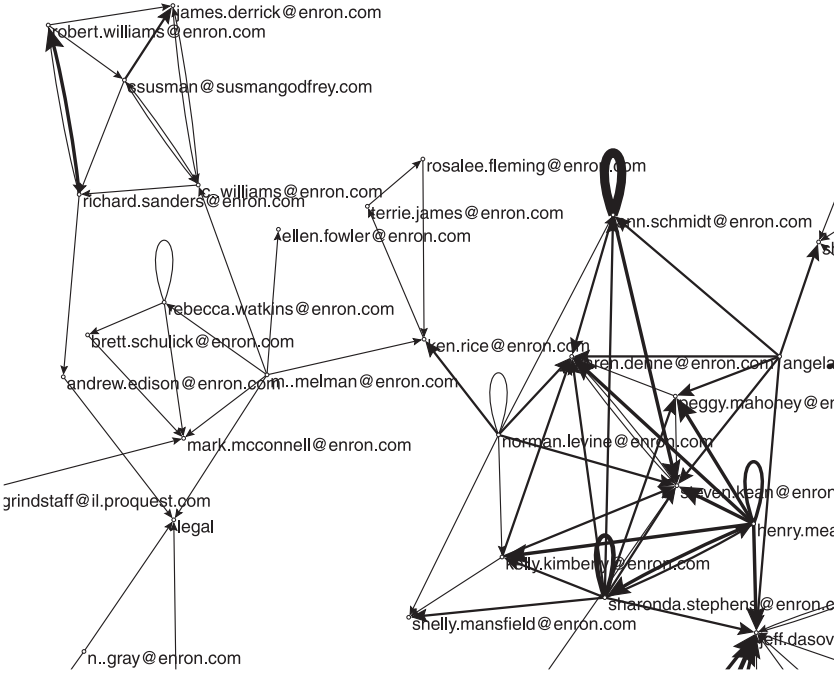
Niet alle onderwerpen die in de onderzoeksmatrix voorkomen, kunnen tegelijk worden opgepakt. Op dit moment zijn er naast het opzetten van het onderwijs drie onderzoeksinitiatieven.

1. Onderzoek naar e-mailfiltering

In 2009 heb ik een artikel gepresenteerd op de DESI III Global E-Discovery Workshop die onderdeel uitmaakte van de 12th International Conference on Artificial Intelligence and Law (Henseler, 2009). In dit artikel beschrijf ik een aantal ideeën om e-mail slimmer te filteren door gebruik te maken van de gestructureerde informatie van e-mail, zoals afzender, geadresseerden en verzenddatum in combinatie met zoekwoorden. Het artikel heb ik inmiddels uitgewerkt met voorbeelden uit de e-mail in de Enron zaak.[8] Een voorbeeld is geconstrueerd aan de hand van 330 e-mails waarin het woord 'Blockbuster' voorkomt. Enron en Blockbuster, een Amerikaanse dvd- en videoketen, kondigden in het jaar 2000 een strategische samenwerking aan. Vervolgens nam Enron toekomstige winsten in de boekhouding op, ook nadat Blockbuster de samenwerking had opgezegd. Figuur 6 laat een sociogram zien waarin de pijlen aangeven welke personen met elkaar contact hebben gehad en hoe vaak.

In sociale netwerkanalyse wordt onderzoek gedaan naar dit soort netwerken. De zogenaamde 'eigenvector centrality' is een bekende maat die gebruikt wordt om het belang van een knooppunt in het netwerk te beoordelen door rekening te houden met het belang van naburige (verbonden) knooppunten. Zoekmachine Google werkt op een vergelijkbare manier door internetpagina's waarnaar veel verwezen wordt een hogere ranking te geven in de resultaatlijst, zodat ze sneller gevonden worden dan pagina's waar minder vaak naar verwe-

zen wordt. De achterliggende gedachte is dat dit soort analyses gebruikt kan worden om de computer slimmer e-mail te laten filteren. Op dit terrein wordt samenwerking gezocht met de afdeling Informatica van de Universiteit van Amsterdam[9], waar niet alleen onderzoek naar sociale netwerkanalyse wordt gedaan, maar ook naar geavanceerde information retrieval technieken.



Figuur 6: Sociogram van Enron medewerkers samengesteld uit gefilterde e-mail

2. Onderzoek naar forensic readiness

Forensic readiness is het tweede onderwerp waar de Kenniskring op dit moment onderzoek naar doet. Het doel hiervan is om een checklist met maatregelen en normen op te stellen aan de hand waarvan bedrijven en organisaties kunnen vaststellen welke problemen ze kunnen verwachten op het moment dat ze te maken krijgen met een E-Discovery project. Dit soort onderzoek is niet nieuw. In het boek *Fraude: preventie en control* (Mikkers en Van Schoten, 2006) wordt forensic readiness gedefinieerd als 'de mate waarin een organisatie die gegevens beschikbaar heeft, die nodig zijn om een fraudeonderzoek uit te kunnen voeren'. De auteurs identificeren een proces in tien stappen, dat

begint bij de identificatie van bedrijfsprocessen waarvoor digitaal bewijs noodzakelijk is. Deze benadering is ontwikkeld vanuit een fraudeperspectief. Het is ook mogelijk om een benadering te kiezen vanuit het perspectief van informatiebeveiliging. Die benadering levert een meer technische checklist op, zoals de uitgebreidere lijst van WareOnEarth Communications Inc.[10]

De Kenniskring kiest voor een aanpak waarbij in eerste instantie bedrijfsprocessen als uitgangspunt gekozen worden, en waarbij in tweede instantie vragen ontwikkeld worden die vergelijkbaar zijn met een checklist die hoort bij de Code van Informatiebeveiliging.[11] Een aantal leden van de Kenniskring heeft kennis en ervaring met de ISO 27001 en 27002 standaard. Vanuit het E-Discovery perspectief zullen zij een begin maken met een 'Code voor forensic readiness'. De Kenniskring wil dit vanzelfsprekend niet alleen doen, maar hier ook bedrijven en andere kennisinstellingen bij betrekken.

Het is ook de bedoeling om studenten via het onderwijs te betrekken in dit onderzoek. Zij zullen in kleine groepjes aan de hand van een checklist een forensic readiness audit uitvoeren en daarover rapporteren. Op die manier willen we feedback krijgen en stapsgewijs komen tot een in de praktijk met studenten geteste checklist en audit-aanpak voor forensic readiness.

3. Ontwikkeling van een E-Discovery onderzoekslab

Voor het studieonderdeel Computer Forensics is al software beschikbaar, en een practicumruimte waar studenten met verschillende forensische tools kunnen werken. De practicumopdrachten zijn gericht op de technische analyse van opslagmedia en besturingssystemen. In dit practicum worden studenten geacht zelf hun onderzoeksomgeving op te bouwen en daarmee technisch diepgaande analyses te doen. Het is de bedoeling om voor het onderzoek naar E-Discovery een operationele omgeving aan te bieden waarin niet alleen forensisch computeronderzoek uitgevoerd wordt, maar waarin alle facetten van E-Discovery onderzocht kunnen worden. Naast de standaardgereedschappen die in de omgeving aanwezig zijn, zal er ook geïnvesteerd worden in de opbouw van standaard datasets (zoals de Enron e-mailverzameling). Er zullen een aantal vaste onderzoekslijnen worden uitgezet, zodat er met behulp van studentenprojecten gebouwd kan worden aan nieuwe deeloplossingen die aan de uitrusting van het E-Discovery lab worden toegevoegd, en later in nieuwe projecten verder verfijnd kunnen worden.

4.3 Onderwijs

Het Lectoraat E-Discovery zal in eerste instantie aansluiten bij de minor Forensic Intelligence en Security (FIS), die in het derde jaar van de voltijdoplei-

ding (Technische) Informatica wordt gegeven. Deze minor is een aantal jaren geleden gestart in de verdiepingsfase, om te voorzien in de groeiende vraag naar specialisten op HBO-niveau op het gebied van forensisch computeronderzoek en computer-security. In het studiejaar 2009/2010 krijgen studenten in de minor FIS voor het eerst de mogelijkheid om, aansluitend op het eerste lesblok computer forensics, te kiezen voor een zelfstandig uit te voeren studieonderdeel E-Discovery, in plaats van een opdracht technische computer forensics.

In het studieonderdeel E-Discovery leren studenten wat E-Discovery inhoudt, wat de problematiek is van de steeds toenemende hoeveelheid digitale informatie, en hoe ze uit de aanwezige digitale gegevens relevante informatie kunnen abstraheren.

E-Discovery in de minor Forensic Intelligence & Security

Het studieonderdeel E-Discovery bestaat uit zeven colleges, en een praktijkopdracht waarbij studenten in paren bij een bedrijf een forensic readiness scan doen op basis van een E-Discovery vragenlijst die door de Kenniskring E-Discovery is ontwikkeld.

Inleiding E-Discovery
Na een korte inleiding in E-Discovery aan de hand van het EDRM krijgen de studenten een overzicht van het vak. In het tweede uur zal een denkbeeldige case gepresenteerd worden om de verschillende E-Discovery onderwerpen in perspectief te brengen. Om zoveel mogelijk tot de verbeelding van de studenten te spreken, is ervoor gekozen om een case in een redelijk bekende bedrijfsomgeving te kiezen, namelijk een ziekenhuis.

Forensic readiness: hoe en waarom, fraude onderzoeken
De Kenniskring E-Discovery zal een 'Code voor forensic readiness' opstellen. Aan de hand van deze code zal een auditmethode ontwikkeld worden (een soort vragenlijst) waarmee onderzocht kan worden in welke mate een bedrijf is voorbereid op E-Discovery werkzaamheden. In het tweede college worden deze code en de bijbehorende auditmethode uitgelegd aan de studenten. Zij worden vervolgens geacht om dit in kleine groepjes bij een bedrijf uit te voeren en de resultaten te rapporteren.

Informatiebronnen in organisaties en bewaarplicht
In dit college wordt in nauwe samenwerking met de opleiding Media, Informatie en Communicatie uitleg gegeven over de betekenis van records

management en de gevolgen (kansen/bedreigingen) voor E-Discovery. Niet alleen bewaarplicht van informatie is van belang, minstens even belangrijk is de plicht om informatie te vernietigen. Een goede records management-strategie kan E-Discovery vereenvoudigen.

Ethische aspecten en de rol van privégegevens
Hoever mag je gaan bij het verzamelen van informatie ten behoeve van een onderzoek? Wat is toegestaan door de wet en wat is ethisch nog verantwoord? In Nederland speelt de Wbp (Wet bescherming persoonsgegevens) een belangrijke rol. Wat houdt die wet in? Hoe wordt die in de praktijk toegepast? Wat is de rol van het CBP (College bescherming persoonsgegevens)? Bij cross-border E-Discovery worden met name de data protection (privacy) problemen groter. De uitlevering van gegevens vanuit Nederland naar een niet-EU land (bijvoorbeeld de VS) staat ter discussie. Wat is het Safe Harbor principe?

E-mail discovery, ontdubbelen van gegevens, information retrieval en text mining
In E-Discovery speelt e-mail een vooraanstaande rol, omdat die bijzonder veel formele en informele correspondentie bevat. In het bekende Enron onderzoek zijn er miljoenen e-mails geanalyseerd. Hoe gaat zo'n analyse in zijn werk? Welke forensische aspecten mogen niet uit het oog verloren worden? Hoe kan een schaalbaar proces opgezet worden, zodat niet alleen de verwerking, maar ook de review door een heel team aangepakt kan worden? Hoe kunnen slimme zoektechnieken en visualisatietechnieken gebruikt worden om sneller relevante informatie te vinden, ook al weet je niet precies wat je zoekt?

Zoeken naar sporen in data warehouses
Grote ondernemingen brengen hun bedrijfsinformatie (inkoop, verkoop, logistiek enzovoorts) onder in zogeheten data warehouses. Bij een grootschalig onderzoek is deze informatie van grote waarde, maar het is niet eenvoudig om in die enorme berg snel relevante informatie te vinden. De standaardsystemen die het bedrijf gebruikt zijn meestal ongeschikt voor dit soort taken. Door informatie uit databases te verzamelen in één nieuwe database kunnen met slimme database queries verbanden gelegd worden die soms leiden tot nieuwe inzichten.

E-Discovery in de praktijk
In het laatste college zal een gastspreker een presentatie geven waarmee E-

Discovery in de praktijk geïllustreerd wordt, en presenteren de studenten de resultaten van hun forensic readiness scan. De resultaten van de praktijkopdrachten zullen met de andere studenten, gastspreker en aanwezige docenten besproken worden.

Naast de voorbereidingen voor het vak E-Discovery in de minor FIS, liggen er bovendien plannen voor de ontwikkeling van een complete E-Discovery minor in de deeltijdopleiding Informatica. Deze minor is ook toegankelijk voor bachelorstudenten van andere opleidingen en zal ook worden aangeboden in de deeltijdopleiding Media, Informatie en Communicatie. Het deeltijdonderwijs is toegankelijk voor professionals uit het bedrijfsleven die meer willen leren over en ervaring willen opdoen met E-Discovery.

Aanvraag Intensief Project E-Discovery

Een Intensief Programma[12] (IP) is een kort studieprogramma dat studenten en medewerkers van instellingen voor hoger onderwijs uit drie of meer deelnemende landen samenbrengt. De Kenniskring E-Discovery zal een aanvraag indienen voor een IP Project E-Discovery dat is gericht op het verwerken en analyseren van e-mails met als voorbeeld de Enron e-mailcollectie (Klimt en Yang, 2004). De Enron e-mailcollectie bevat in totaal meer dan 500.000 e-mails uit de mailboxen van 150 Enron medewerkers. Deze verzameling is al uitgebreid onderzocht en op het internet is er veel over te vinden.

Door middel van dit IP-project zal de Kenniskring op een efficiënte manier internationale contacten kunnen leggen met buitenlandse hogere onderwijsinstellingen die ook geïnteresseerd zijn in het thema E-Discovery. Overigens is het leuke van een IP dat studenten en docenten in staat worden gesteld om in multinationale groepen samen te werken en op die manier te profiteren van speciale leer- en lesomstandigheden die in de afzonderlijke instellingen niet beschikbaar zijn, zodat hun blik ten aanzien van het studieonderwerp verruimd wordt. Belangrijk voor zowel onderzoek als onderwijs is dat docenten de mogelijkheid geboden wordt om met buitenlandse collega's van gedachten te wisselen over vakinhoudelijke kwesties en curriculumontwikkeling, en om nieuwe onderwijsmethoden in een internationale onderwijsomgeving te testen.

Gelet op de vele EU-initiatieven op het terrein van fraudebestrijding[13] en concurrentiebeleid[14], de richtlijn tegen corruptie[15], en de bewezen relevantie van E-Discovery voor deze terreinen, acht ik de kans groot dat ons IP-voorstel

zal worden geaccepteerd en zullen wij naar verwachting begin 2011 de eerste editie van dit project uitvoeren.

4.4 Samenwerking met overheid en bedrijfsleven

Een van de doelen van het lectoraat is het opzetten van een netwerk van kennisinstellingen, dienstverleners en gebruikers van kennis op het gebied van E-Discovery. Wij willen dit doel realiseren door een platform te creëren waarin met zowel de overheid als het bedrijfsleven wordt samengewerkt. In onderstaande tabel worden de verschillende soorten spelers in deze groepen benoemd.

	Dienstverleners en gebruikers	Kennisinstellingen	Afnemers
Bedrijfsleven	Advocatuur, forensische accountants, particuliere onderzoeksbureaus	Ontwikkelaars van E-Discovery software en diensten	Bedrijven
Overheid	Toezichthouders en (bijzondere) opsporingsdiensten	Researchinstellingen met expertise op E-Discovery (deel)gebieden	(Semi-)overheidsorganisaties

Tabel 2: Een netwerk van kennisinstellingen

Hieronder zal ik kort toelichten wat het belang van elk van deze groepen is en welke rol zij in een platform voor E-Discovery zouden kunnen spelen.

Advocatuur, forensische accountants en particuliere onderzoeksbureaus

Advocatuur, forensische accountants en particuliere onderzoeksbureaus hebben behoefte aan goede E-Discovery gereedschappen en algemeen geaccepteerde protocollen om digitaal bewijs te verzamelen, te verwerken en te analyseren. Enerzijds voorzien zij zelf in die behoefte door eigen kennis te ontwikkelen, maar door het multidisciplinaire karakter van E-Discovery is het juist belangrijk om verschillende invalshoeken uit de advocatenpraktijk, de forensische accountancy en particulier onderzoek te combineren.

Ontwikkelaars van E-Discovery software en diensten

Ontwikkelaars van E-Discovery software en diensten kunnen een belangrijke bijdrage leveren aan de beheersbaarheid van E-Discovery problemen, maar voorwaarde daarvoor is wel dat zij dicht bij de praktijk staan. Sommige softwareontwikkelaars onderkennen dit en bieden ook diensten aan op basis van hun eigen E-Discovery software. Door diensten niet alleen te ontwikkelen maar ook aan te bieden, worden ze vanzelf beter en wordt ook de onderliggende software verbeterd. De achterliggende gedachte is goed, maar gebruikers willen liever niet afhankelijk zijn van één aanbieder. Een platform waarin ontwikkelaars samen met gebruikers kennis en ervaring delen zal op een meer onafhankelijke manier de kwaliteit van de aangeboden software en diensten verhogen.

Toezichthouders en bijzondere opsporingsdiensten

Toezichthouders en bijzondere opsporingsdiensten kunnen bij E-Discovery baat hebben bij feedback van advocaten, forensische accountants en particuliere onderzoekers, die zij tegenkomen in hun onderzoeken bij bedrijven. Nu gebeurt dat ad hoc en tijdens een onderzoek, waardoor er vaak spanningen zijn die een open en ongedwongen samenwerking in de weg staan. Sommige toezichthouders doen een poging om via mantelovereenkomsten tot een productieve samenwerking te komen, maar hier ligt toch meestal de nadruk op dichtgetimmerde contractuele verplichtingen en is er weinig ruimte voor een open dialoog. Ook de relatie tussen overheid en ontwikkelaars van E-Discovery software is tweeslachtig. Mogelijk is er sprake van de wet van de remmende voorsprong. In de jaren '90 en begin 2000 kregen toezichthouders en bijzondere opsporingsdiensten al te maken met E-Discovery problemen, terwijl de aangeboden software deze problemen slechts gedeeltelijk oploste. Het is logisch dat deze organisaties aan de slag zijn gegaan om zelf hun problemen op te lossen. Pas in de laatste jaren wordt functionaliteit voor het forensisch kopiëren van informatie, het doorzoeken en het reviewen geïntegreerd aangeboden. Inmiddels zijn er binnen de overheid diverse eigen E-Discovery oplossingen ontwikkeld waar men (nog) geen afscheid van wil nemen. Zulke oplossingen zijn echter duur om te onderhouden en beginnen langzaam achter te lopen bij de commercieel beschikbare oplossingen.

Researchinstellingen met expertise op E-Discovery (deel)gebieden

Researchinstellingen zijn in veel gevallen op zoek naar toepassingsmogelijkheden van de kennis die zij hebben ontwikkeld. Op dit moment zijn er geen uit-

gesproken E-Discovery researchgroepen, tenminste niet in Nederland. Nederland kent echter wel een sterke traditie op het gebied van informatiemanagement en intelligente automatische verwerking van informatie (taaltechnologie, information retrieval, data mining, text mining, artificial intelligence enzovoorts). Voor groepen die zich op deze terreinen bezighouden, is E-Discovery een kans om nieuwe technieken in de praktijk te toetsen. Ik verwacht dat er van deze groepen oplossingen komen die onderdelen van het privacyprobleem kunnen oplossen door software te maken waarmee de computer nog beter informatie automatisch kan filteren, zodat niet onnodig veel informatie door mensen onderzocht hoeft te worden.

Bedrijven en (semi-)overheidsorganisaties die E-Discovery diensten afnemen

Ten slotte zijn er bedrijven en (semi-)overheidsorganisaties die hun elektronische informatie beter willen voorbereiden op interne of externe onderzoeken. Zij zijn voornamelijk klanten van de hierboven genoemde dienstverleners of zijn het doelwit van eerdergenoemde toezichthouders. In het kader van forensic readiness kan de Kenniskring in samenwerking met deze partijen in een snel en praktijkgestuurd proces een code voor forensic readiness ontwikkelen. Andersom zullen deze partijen vooral op het gebied van forensic readiness veel zelf kunnen doen en daarom op hun beurt ook geïnteresseerd zijn in samenwerking op dit terrein.

E-Discovery software

Grote spelers in de markt voor enterprise search en records management hebben zich de afgelopen jaren versterkt om in te kunnen spelen op de vraag naar E-Discovery oplossingen. Een voorbeeld daarvan is de overname enkele jaren geleden van de firma Zantaz door Autonomy. Zantaz was oorspronkelijk gespecialiseerd in e-mail archiving oplossingen en heeft zich ontwikkeld tot een belangrijke speler in het E-Discovery veld. Autonomy heeft nu een belangrijke uitgangspositie om bestaande corporate klanten te benaderen met een E-Discovery oplossing die naadloos aansluit (althans dat wordt beweerd) op de bestaande content management en enterprise search systemen. Een belangrijke stap, want Autonomy zit nu gevangen tussen Google en Microsoft, terwijl die laatste met de acquisitie van FAST Technologies grote stappen zet op de enterprise search markt.

Een ander interessant voorbeeld is de overname vorig jaar van Stratify door Iron Mountain. Iron Mountain is wereldwijd bekend als de aanbieder van oplossingen en diensten voor opslag, management en bescherming van archieven, media en elektronische gegevens. Bijna iedereen kent de blauwwitte archiefdozen van Iron Mountain, waarin de statische dossiers zorgvuldig worden gearchiveerd en extern worden opgeslagen. Inmiddels biedt Iron Mountain ook software en diensten aan om PC's via het internet te back-uppen. Stratify is een Amerikaans bedrijf dat E-Discovery diensten aanbiedt en is vooral bekend vanwege de geavanceerde review oplossing waarmee klanten via het internet grote verzamelingen e-mails kunnen reviewen. De overname van Stratify door Iron Mountain is strategisch een slimme zet, omdat het traditionele records management en E-Discovery naadloos op elkaar aansluiten.

De bedrijven Guidance en AccessData zijn bekend vanwege hun computer forensic tools. Beide producten zijn erg populair bij politie, opsporingsdiensten, forensische accountants en particuliere onderzoeksbureaus. Guidance maakt het product Encase en AccessData is de maker van Forensic Toolkit. Vroeger werd Encase vooral gebruikt voor het maken van een forensische computer image. Dat wil zeggen dat niet alleen de bestanden worden gekopieerd maar ook ruimte op de harde schijf die niet in gebruik is, maar mogelijk wel in gebruik is geweest. Forensic Toolkit was het product met meer functies om een snel onderzoek te doen op zo'n forensische kopie, bijvoorbeeld door een full-text search index te maken. Tegenwoordig overlapt de functionaliteit van deze producten grotendeels. Bovendien hebben beide een enterprise editie van hun software, waarmee grote bedrijven hun eigen E-Discovery projecten kunnen uitvoeren.

Toch bieden zowel de producten van Guidance als die van AccessData nog geen oplossing voor grootschalige E-Discovery projecten. De hoeveelheid informatie is dusdanig groot dat het verzamelen en verwerken soms wel weken of maanden kan duren. In dat geval wordt met verscheidene tools een zogenaamde digitale wasstraat opgezet waarmee verschillende verwerkingsstappen continu worden uitgevoerd, zodat informatie in kleinere batches verwerkt kan worden. Het voordeel is dat de handmatige analyse van de verwerkte informatie al kan beginnen, terwijl nog niet alle informatie verwerkt is. Leveranciers als iPro, LexisNexis en OutIndex maken software die prima op onderdelen van de digitale wasstraat kan worden ingezet om data te verwerken. Weer andere leveranciers, zoals iCONECT, FTI en Concordance, leggen de nadruk meer op het reviewen van informatie en proberen hun tools steeds slimmer te maken door informatie automatisch te groeperen en verbanden te leggen. Ook hier is duidelijk zicht-

baar dat met de groeiende vraag naar E-Discovery oplossingen leveranciers steeds meer functionaliteit aanbieden om te voorkomen dat hun gebruikers overstappen op het product van hun concurrent.

Het is zeker niet zo dat E-Discovery software alleen in het buitenland gemaakt wordt. Het Amsterdamse softwarebedrijf ZyLAB bestaat al meer dan 25 jaar en ontwikkelt E-Discovery en records management software die al sinds het begin van de jaren '90 door politie en bijzondere opsporingsdiensten wordt gebruikt voor het doorzoeken van elektronische informatie.

Net als de eerdergenoemde leveranciers breidt ook ZyLAB constant de functionaliteit van de aangeboden software uit. In de periode 2000-2006 heb ik als technisch directeur bij ZyLAB een belangrijke bijdrage mogen leveren aan uitbreiding van de ZyLAB software van krachtig zoekprogramma tot een geïntegreerde duurzame oplossing voor het verwerken en beheren van elektronische bestanden en papieren documenten inclusief text mining, visualisatie en een web-based platform om bewijsmateriaal te reviewen. Sinds een aantal jaren wordt ZyLAB door analist Gartner als leider gezien in de markt van information access software. Ook analist IDC en het gerenommeerde tijdschrift Knowledge Management World zijn onder de indruk van de E-Discovery software van ZyLAB.

Conclusie en dankwoord

We naderen het einde van deze openbare les. Er valt nog veel meer te vertellen, te leren en zeker ook te ontdekken op het gebied van E-Discovery. In het begin van deze openbare les heb ik de E-Discovery ontwikkelingen laten zien in de loop van de afgelopen twintig jaar. Via een aantal verschillende perspectieven op E-Discovery heb ik uiteindelijk een agenda gepresenteerd voor het lectoraat. Een agenda die uitdagend toegepast E-Discovery onderzoek bevat, en waarin ik beschrijf hoe dit onderzoek gecombineerd kan worden met nieuw onderwijs in verschillende opleidingen binnen het Domein Media, Creatie en Informatie.

Onze zoektocht naar de digitale werkelijkheid is pas net begonnen. Een lectoraat kan zoiets niet alleen en daarom wordt samenwerking gezocht met overheid en bedrijfsleven, zoals ik in het slot van het vorige hoofdstuk uiteengezet heb.

Ook een openbare les komt niet zonder samenwerking tot stand. Daarom wil ik mijn dank uitspreken aan allen die mij hierbij geholpen hebben. Allereerst wil ik de leden van de Kenniskring E-Discovery bedanken: Carla Bombeld, Geert-Jan van Bussel, Arnim Eijkhoudt, Karel Pieterson, Theo Ris en Ellen Waterman. Zowel voor het gezamenlijk invullen van de onderzoeksagenda als voor het vormgeven van E-Discovery onderwijs in het afgelopen jaar, en ook voor hun waardevolle aanvullingen en opmerkingen op eerdere versies van deze openbare les. Janet Hofstra wil ik bedanken voor haar administratieve ondersteuning van de Kenniskring. Dank aan mijn medelectoren Guus Delen, Jacob Brunekreef en Ben Kröse, die mij op sleeptouw hebben genomen in de verschillende domeininitiatieven waarbij input van de lectoren gevraagd wordt. Ook dank aan lectoren Geert Lovink en Joost Kircz omdat mede door hun lectoraten het onderwerp E-Discovery vanuit het perspectief van interactieve media en informatiemanagement nog breder benaderd kan worden. Opleidingsmanager Kees Rijsenbrij wil ik bedanken voor zijn niet-aflatende steun en aandacht voor E-Discovery en voor zijn commentaar op de conceptversie van deze openbare les.

Voorts wil ik PricewaterhouseCoopers Advisory NV bedanken, en in het bijzonder André Mikkers en Bernard Prins, voor de mogelijkheid die ze mij bieden om mijn werkzaamheden als lector te combineren met mijn werk als director bij PwC. Mijn collega's van de Forensic Technology Solutions groep wil ik bedanken voor de uitstekende samenwerking en de goede sfeer. Het is werkelijk een plezier om met jullie samen te werken. Zonder jullie inzet zou het een stuk moeilijker zijn om zoveel tijd aan de Hogeschool te besteden. Naarmate het lectoraat zich ontwikkelt en de eerder beschreven samenwerking gestalte krijgt, verwacht ik jullie meer hierbij te kunnen betrekken.

Ten slotte wil ik mijn vrouw Jolanda en mijn zoons Rutger en Matthijs bedanken. Lieve Jola, bedankt voor je geduld en voor het doorlezen en corrigeren van de teksten voor deze openbare les, terwijl je naast je werk en ons gezin het ook nog druk hebt met je opleiding. De volgende kerstvakantie nemen we echt vrij!

Noten

1. De Wet van Kryder is minder hard geformuleerd dan de Wet van Moore. De *Scientific American* heeft een interessant artikel over de ontwikkelingen op het gebied van diskopslag en de rol van Mark Kryder. Zie http://www.scientificamerican.com/article.cfm?id=kryders-law.
2. Op internet zijn vele informatiebronnen te vinden die een visie geven op de FRCP. Wikipedia is een van de bronnen: http://en.wikipedia.org/wiki/Federal_Rules_of_Civil_Procedure.
3. Voor meer informatie over de herziene digitale werkwijze, zie de website van de NMa op http://www.nmanet.nl/nederlands/home/Actueel/Publicaties/Richtsnoeren/NMa_herziet_werkwijze_digitaal_onderzoek.asp.
4. Meer informatie over de FCPA is te vinden op de website van het Amerikaans Ministerie van Justitie: http://www.justice.gov/criminal/fraud/fcpa/.
5. De elektronische versie van de Economic Crime Survey 2009 kan gedownload worden van de website van PwC: http://www.pwc.com/gx/en/economic-crime-survey/index.jhtml.
6. Voor meer informatie over deze conferentie, zie de website: http://www.corporateaccountability2009.com/CAC09%20Amsterdam/amsterdam.html.
7. De activiteiten van The Sedona Conference worden bijgehouden op de volgende website: http://www.thesedonaconference.org.
8. De uitgebreide versie van het DESI-III paper is ter publicatie in het special issue over E-Discovery ingediend bij het tijdschrift *Artificial Intelligence and Law*.
9. Zie ook de website van de Information and Language Processing Systems groep: http://ilps.science.uva.nl/, en researchpublicaties van Prof. Maarten de Rijke en zijn medewerkers: http://staff.science.uva.nl/~mdr/Research/index.html.
10. Digital Forensics Readiness Checklist: http://www.wareonearth.com/resources_forensics.html.
11. NEN norm NEN-ISO/IEC 27002:2007.
12. Zie ook de Intensive Programmes website van het Nuffic: http://www.nuffic.nl/nederlandse-organisaties/services/beursprogrammas/lll-erasmus/intensive-programmes/intensive-programmes-2009-2010/intensive-programmes-2009-2010.
13. Meer informatie over de EU-aanpak van fraudebestrijding is te vinden op de website van de EU: http://europa.eu/legislation_summaries/fight_against_fraud/anti_fraud_offices/index_en.htm.
14. Meer informatie over de EU-aanpak van mededingingsonderzoeken is te vinden op de website van de EU: http://ec.europa.eu/competition/index_en.html.
15. Meer informatie over de EU-aanpak in de bestrijding van corruptie is te vinden op de website van de EU: http://europa.eu/legislation_summaries/fight_against_fraud/fight_against_corruption/l33301_en.htm.

Literatuur

Boon, V. van der, 'Actie tegen vastgoedfraude', in *Het Financieele Dagblad*, 14 november 2007.

Boon, V. van der en Maarel, G. van der, *De Vastgoedfraude*, uitgave van *Het Financieele Dagblad*, 2009.

Fox, L., *Enron: The Rise and Fall*, John Wiley & Sons, Inc., 2003.

Gantz, J.F., Reinsel, D., Chute, C., Schlichting, W., Mcarthur, J., Minton, S., Xheneti, I., Toncheva, A., Manfrediz, A., 'IDC – The Expanding Digital Universe: A Forecast of Worldwide Information Growth Through 2010', in *IDC Whitepaper*, http://www.idc.com, maart 2007.

Henseler, H., 'Georganiseerde misdaad is goed geautomatiseerd', in de *Automatisering Gids* 52, 30 december 1994.

Henseler, H., 'Computer Crime and Computer Forensics', in: Jay Siegel, ed., *Enceclopedia of Forensic Sciences*, London Academic Press, 2000.

Henseler, H., 'Network Based Filtering For Large E-Mail Collections in E-Discovery', *Proceedings of the DESI III Workshop, ICAIL*, Barcelona 2009, http://www.law.pitt.edu/DESI3_Workshop/Papers/DESI_III.HansHenseler.pdf.

Klimt, B. en Yang, Y., 'Introducing the Enron Corpus', *Proceedings of the Collaboration, Electronic Messaging, Anti-abuse and Spam Conference*, 2004, http://www.ceas.cc/papers-2004/168.pdf.

Mikkers, A. en Schoten, E. van, *Fraude, preventie en control*, Kluwer, 2006.

Moore, G. E., 'Cramming more components onto integrated circuits', in *Electronics* vol. 38, no. 8/1965, ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf.

Pous, V. de, 'Digitaal bewijs weggooien mag niet meer', in de *Automatisering Gids*, 2 maart 2007.

The Sedona Conference, 'Sedona Principles Rapport', *The Sedona Conference*, *WG1*, 2003. http://www.thesedonaconference.org/dltForm?did=SedonaPrinciples200303.pdf.

The Sedona Conference, 'The Sedona Principles after the Federal Amendments: The Second Edition', *The Sedona Conference, WG1*, 2007a.

The Sedona Conference, 'Sedona Guidelines', *The Sedona Conference, WG1*, 2007b, http://www.thesedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf.

The Sedona Conference, 'Best Practices Commentary on Search & Retrieval Methods', *The Sedona Conference, WG1*, 2007c. http://www.thesedonaconference.org/dltForm?did=Best_Practices_Retrieval_Methods_revised_cover_and_preface.pdf.

The Sedona Conference, 'Framework for Analysis of Cross-Border Discovery Conflicts', *The Sedona Conference*, 2008, http://www.thesedonaconference.org/dltForm?did=WG6_Cross_Border.

The Sedona Conference, 'The Sedona Conference Commentary on Achieving Quality in the E-Discovery Process', *The Sedona Conference, WG1*, 2009, http://www.thesedonaconference.org/dltForm?did=Achieving_Quality.pdf.

Curriculum vitae

Hans Henseler is geboren in 1964 en heeft Informatica gestudeerd aan de TU Delft van 1982-1987. Aansluitend is hij als onderzoeker gaan werken aan de Rijksuniversiteit Limburg bij de vakgroep Informatica. In 1993 is hij gepromoveerd op het onderwerp artificiële neurale netwerken en patroonherkenning. In 1992 is hij in dienst getreden als forensisch computeronderzoeker bij het Gerechtelijk Laboratorium in Rijswijk, waar hij de afdeling Forensisch Computer Onderzoek heeft opgezet. In het kader van zijn werk als forensisch onderzoeker heeft hij samengewerkt met inlichtingen- en opsporingsdiensten in binnen- en buitenland en is hij van 1996-1997 vicevoorzitter geweest van de International Organisation of Computer Evidence. Naast vele presentaties op uiteenlopende conferenties in binnen- en buitenland heeft hij ook een groot aantal publicaties in tijdschriften en boeken op zijn naam staan, waaronder een artikel in de Encyclopedia of Forensic Sciences getiteld 'Computer Crime'. Van 1998 tot 2000 was hij leider van de divisie Informatiesystemen van TNO TPD, waarin specialismen zaten op het gebied van informatiesystemen, natuurlijke taalverwerking, kennismanagement en digitale beeldbewerking. Van 2000 tot en met 2006 was hij als technisch directeur van ZyLAB verantwoordelijk voor de ontwikkeling van standaardsoftware voor documentmanagement, records management en E-Discovery. Sinds eind 2006 is Hans Henseler werkzaam bij PricewaterhouseCoopers Advisory NV (PwC) op de afdeling Dispute Analysis & Investigations. Hij is director Forensic Technology Solutions (FTS) in het PwC Central Cluster en is verantwoordelijk voor de acquisitie en uitvoering van onderzoeken en de ontwikkeling en aansturing van circa vijftig forensische specialisten in continentaal West-Europa. Hij heeft onder andere gewerkt aan E-Discovery projecten bij Siemens en MAN in Duitsland, bij Rabo Bouwfonds in het interne onderzoek naar de vermeende vastgoedfraude en recentelijk ook bij het in kaart brengen en verzamelen van digitale informatie ter ondersteuning van de curatoren bij de DSB bank. Sinds 1 januari 2009 is hij parttime Lector E-Discovery aan de Hogeschool van Amsterdam.