

De harde schijf als



De digitale rechercheurs stelden
onmiddellijk de data van de ver-
dachte veilig

corpus delicti

Ook criminelen hebben thuis vaak een pc met internetverbinding staan. Resultaat: een groeiende vracht elektronisch bewijsmateriaal. Om dat te verwerken zijn digitaal-rechercheurs nodig. Een fictief scenario van een zedenzaak .

George van Hal

Rechercheur B. Bauwer van het interregionale bureau digitale expertise had meteen al een voorgevoel dat dit een grotere zaak was dan het zoveelste treurige incident waarbij ene Ome Jan niet met z'n vingers van Pietje van zes af had kunnen blijven. De computer en mobiele telefoon die hij in diens woning aantrof konden wel eens bewijs bevatten voor meer dan alleen ontucht. "Stel, dat ding staat vol met kinderporno," dacht hij. "Waarschijnlijk is er dan ook vanaf zijn pc en mobieltje communicatie geweest met anderen. Met een beetje geluk rollen we een heel kinderporno-netwerk op."

Zoals al Bauwers zaken, was ook deze begonnen met een incident, want of hij dit nu terecht vond of niet, hij werkte slechts reactief en ondersteunend. Pas als een misdrijf een IT-component had, werd de digitale recherche erbij geroepen. Het digitale equivalent van de surveillerende agent bestond nog niet – hoe moest je de bovenbazen duidelijk maken dat het loonde om in werktijd urenlang te gaan zitten googlen en web-surfen?

Nu waren ze dus afhankelijk van types als ome Jan die op een domme manier in de fout gingen en zo de bal aan het rollen brachten.

"Vroeg of laat maken zulke types altijd een domme fout," zei hij minimaal tegen z'n hulpje Peter Redijker, digitaal-rechercheur in opleiding, die al met z'n jas aan in de deuropening stond om huiszoeking te gaan doen. Lang was hij met z'n activiteiten een roepende in de woestijn geweest, maar tegenwoordig bestond er zelfs een speciale MBO-opleiding voor. Volgens Bauwers schatting was er wel plaats voor vierhonderd digitaal rechercheurs bij de Nederlandse politie.

Aangekomen in het morsige galerijflatje van Ome Jan, was Bauwer maar net op tijd om met een luidkeels "Afblijven!" te verhinderen dat zijn assistent de computer in de woonkamer aanzette. "Eerste prioriteit is altijd om de informatie op de computer en telefoon veilig te stellen," doceerde Bauwer nadrukkelijk aan de bedremmelde Redijker. "Als je een kamer binnenkomt en er ligt een lijk met een mes in z'n rug, dan blijft iedereen wel met z'n vingers van het mes af, want iedereen kijkt naar CSI en weet dus dat daar vingerafdrukken of DNA-spooren op kunnen zitten. Maar als het om digitale sporen gaat, gaat iedereen er juist wél met z'n vingers aanzitten."

"Maar we moeten toch nagaan of hij kinderporno heeft gedownload? Hoe wil je dat doen zonder z'n computer op te starten?"

"Dat is dus het domste wat je kunt doen, want je vernietigt sporen. Iedere keer dat je een computer opstart, worden gegevens naar de harde schijf geschreven en cruciale gegevens kunnen dan dus overschreven worden. Bovendien is de integriteit van het onderzoeksmateriaal niet meer gewaarborgd. Je kunt dan gewoon zien dat iemand heeft zitten rommelen in het systeem nadat het onderzoek gestart is, en daar weet de verdediging wel raad mee."

Slackspace Het was eigenlijk een klein wonder, overwoog Bauwer, dat de overige politieagenten in het flatje de elektronica tot nu toe met rust gelaten hadden. Hij liet Redijker meekijken met de vaste procedure om digitale gegevens veilig te stellen: "We starten de pc van de verdachte niet meer op, dat spul wordt allemaal gekopieerd en daar gaat dan een *hash* overheen. Als je ooit iets wijzigt in onderzoekgegevens en je doet weer een hash-

test, dan zul je nooit meer dezelfde waarde krijgen". Zo'n unieke hash-waarde wordt geproduceerd door een ingewikkelde formule waar alle nullen en enen op de harde schijf ingestopt worden. De formule is zodanig geconstrueerd, dat zelfs het veranderen van een enkele nul of één al een compleet ander getal oplevert. "Je doet daarom altijd onderzoek op de kopie en niet op het origineel."

Bauwer haalde daarom de harde schijf uit de computer en sloot die aan op een apparaat waarmee hij rechtstreeks alle data kon kopiëren. Dus niet alleen alle bestanden, maar ook de 'lege' ruimte. Zodra het kopiëren klaar was, werd automatisch de hash-waarde berekend. Hetzelfde deed Bauwer met de USB-stick die naast de computer lag. Bovendien nam hij ome Jans mobiele telefoon mee, en kopieerde ook de data die daar op stonden. Meteen gingen ze terug naar het bureau om het bewijsmateriaal te doorzoeken.

"Er staat bijna niks op die harde schijf," constateerde Redijker al na een minuut of vijf teleurgesteld. "Hij wist natuurlijk dat hij opgepakt zou worden en heeft alles wat maar enigszins tegen hem gebruikt kon worden gewist."

"Werkelijk?," zei Bauwer met een superieur glimlachje. Hij schoof Redijker opzij en ging zelf aan de slag met het materiaal. Een kwartier later had hij honderden fragmenten 'gewiste' informatie boven water gehaald, waarvan de bestandsnamen soms weinig te wenssen over lieten.

"Een harde schijf is opgedeeld in clusters," legde hij aan Redijker uit, "de kleinste geheugeneenheid die nog door het besturingssysteem kan worden aangesproken. Wanneer die clusters tien kilobyte groot zijn en je een tekstbestand opslaat van honderd kilobyte, zijn

dus tien clusters nodig. Als je dat woordbestand wist, haal je alleen de verwijzing ernaar weg, zodat het besturingssysteem weet dat de gegevens niet meer nodig zijn en er eventueel iets overheen mag. Maar de nullen en enen blijven op de schijf aanwezig totdat dat gebeurt – en dat weet niet iedereen.”

“Wanneer nu een nieuw bestand aanmaakt wordt van 82 kilobyte, krijg je geen 8,2 maar negen clusters toegewezen, want kleiner dan een cluster is er niet. In dat negende cluster staat vervolgens twee kilobyte van het nieuwe bestand, maar nog steeds acht kilobyte van het oude bestand. Dat heet met een mooi woord *slackspace*. Het tiende cluster is nog helemaal gevuld met het oude bestand en heet *freespace*.”

Uit die *slack-* en *freespace* haalde Bauwer met zijn recherchesoftware delen van Ome Jans gewiste bestanden op. “Omdat harde schijven steeds groter worden en de clusters in het echt groter zijn dan tien kilobyte, vind je heel veel informatie terug”, zei hij. “Je slaat zo vreselijk veel op dat sporen goed wissen heel moeilijk is.”

Tekenfilm De deur van Bauwers kantoorje zwaaide open. “Heb je die vieze plaatjes al doorgekeken? Gaat het nog wat opleveren voor het dossier?” Commissaris Jansen viel als gewoonlijk met de deur in huis. “Nee chef”, vertelde Bauwer, “ik heb al zes gigabyte mogelijk illegaal spul van z’n harde schijf gevestigd, maar misschien is er nog veel meer. De doorsnee kinderporno-verdachte heeft tegenwoordig ongeveer zevenhonderd gigabyte aan foto’s en filmpjes. Voordat we dat allemaal verwerkt hebben, zijn we wel een aantal dagen verder.”

“Dat kan tegenwoordig toch allemaal automatisch?”, antwoordde Jansen korzelijk. “Je matcht de hele handel met die landelijke , hoe heet dat, die coke- nee hash-database. Dacht ik dat

we dat systeem nu eindelijk eens aan de praat hadden, schieten we er blijkbaar nog niks mee op.”

Bauwer sloot even theatraal de ogen, terwijl hij achterover leunde in zijn stoel. Inderdaad waren er tegenwoordig mogelijkheden om de werklast wat in te dammen. “Er is een landelijke hash-database met codes van bekende afbeeldingen”, zei hij, zich nadrukkelijk niet tot Jansen, maar tot Redijker wendend. “Veel van het materiaal dat op internet uitgewisseld wordt, is al wat ouder en is daarom bij ons bekend. Die treffers worden er door het automatische systeem wel uitgefilterd. Een probleem is dat plaatjes soms veranderd zijn, en dan hebben ze niet meer dezelfde hash-waarde. Sowieso zijn de afbeeldingen uit de slack- en freespace niet compleet, of het zijn uitsneden of ze hebben een veranderde kleurdiepte.”

“Zulke details laat ik graag aan jullie, techneuten, over”, mengde Jansen zich weer in het gesprek. De deur uitlopend riep hij nog: “Als er maar resultaat komt, en snel.”

Bauwer zag bij nader inzien af van een laatste woord en startte zijn nieuwste aanwinst op: software die ook van bewerkte plaatjes aangaf of ze op een al bekende afbeelding leken. Zo bleek al snel dat een groot gedeelte van het teruggevonden materiaal, achtduizend afbeeldingen in totaal, inderdaad al bekende kinderporno was.

De dagen daarna bekeken Bauwer en Redijker met eigen ogen alle overige plaatjes, een moeizame taak waarmee doorgaans een derde tot een kwart van de werktijd van een digitaal rechercheur heen ging. Was het kinderporno, dan voegden ze het materiaal toe aan de database om het zoeken de volgende keer te versnellen.

De commissaris kwam ondertussen meermalen per dag binnen lopen: “Zijn we al zover dat we tot arrestaties



over kunnen gaan?” Bauwer hield hem op afstand door te verwijzen naar de afdeling jeugd- en zeden-zaken. Op twintig plaatsen in Nederland zaten rechercheurs van die afdeling elke dag opnieuw naar grotendeels dezelfde walgelijke films te kijken. Zij moesten ook alle films die Ome Jan verzameld had nakijken op nieuw materiaal.

“Wees maar blij dat we dat niet zelf hoeven doen, Redijker”, zei Bauer. “Je geest doet rare dingen met het verwerken van dat soort beelden. Zelfs een specialist loopt altijd de kans ‘af te breken’ en dan voor een hele tijd naar huis te gaan met posttraumatische stress.”

“Waarom wordt op filmpjes niet ook een hashstelsel toegepast? Dan hoeft je ze niet allemaal af te kijken”, vroeg Redijker. “Helaas is dat voor filmpjes niet zo makkelijk te realiseren”, legde Bauer uit. “In theorie is het simpel: kinderpornovideo’s worden vaak vanuit oude analoge banden gedigitaliseerd en dan op internet uitgewisseld. Op die manier zou je dus, net als bij de afbeeldingen, ook een lijst met bekende films moeten kunnen maken. Maar pedofielen en criminelen passen meestal zelf bewerkingen toe op het materiaal. Soms lijkt het een onschuldige tekenfilm, en komt er pas na vijf minuten een kinderporno-scène. Dan gaat zo’n vent met een jochie op de bank zitten om naar de tekenfilm te kijken. Als dan plotseling die porno-



allemaal met een enorme *gun* op de foto te staan. Dan maak je het ons natuurlijk wel erg makkelijk.”

Het kinderporno-netwerk dat ze via ome Jan op het spoor waren gekomen, bleek gaandeweg het onderzoek van vele markten thuis. Een zeer lucratieve bedrijfstak was afpersing. Navraag leerde, dat sommige van die zaken al behandeld waren door particuliere digitaal-recherchebureaus. “Bedrijven stappen in zo’n geval vaak liever naar een particulier dan naar de politie”, zei Bauwer tegen Redijker. “Stel je voor, een stel hackers, of hoe je ze ook wilt noemen, kraakt een website en dreigt naar de pers te stappen. Op zich niet erg, tenzij je als bedrijf van je it-inkomsten afhankelijk bent. Stel dat bekend wordt dat kwaadwillenden hebben ingebroken in de internetbankierservice van een grote bank. Dan heeft die bank een flink probleem, omdat klanten het toch al precaire vertrouwen in de service verliezen.”

Wapenwedloop “Puur technisch bekeken, hebben die pedofielen dat knap gedaan,” moest Bauwer toegeven, toen hij Redijker demonstreerde hoe de leden van het kinderporno-netwerk anoniem bestanden uitwisselden. “Ze weten er duidelijk meer van dan de Hofstadgroep. Die dachten al dat ze geen sporen meer achter zouden laten door hun MSN-verkeer te versleutelen.”

Als digitaal rechercheur kreeg Bauwer niet vaak te maken met technisch geavanceerde tegenstanders, dus was dit een kolfje naar zijn hand. “We zijn feitelijk in een wapenwedloop verwickeld, want de technieken van onze afdeling moeten in de rechtszaal meestal bekend gemaakt worden om verdachten veroordeeld te krijgen. We leiden dus eigenlijk onze eigen criminelen op, Redijker.”

De tijden waren al lang voorbij dat wachtwoorden om versleutelde bestanden met kinderporno te bekijken,

scène komt, kan hij zien hoe dat jochie erop reageert.”

Bauwers grootste nachtmerrie was, dat zijn afdeling ooit materiaal in beslag zou nemen waarop een kind te zien was waarvan het misbruik nog steeds aan de gang was, en dat ze het over het hoofd zouden zien. Er zat voor de zedenrechercheurs dus niets anders op, dan al het materiaal van begin tot eind te bekijken.

Inmiddels werd wel gewerkt, samen met de Universiteit van Amsterdam, TNO en een commerciële partij, aan software die de inhoud van filmbeelden kon herkennen. “Wat zou het mooi zijn,” filosofeerde Bauwer, “als je een computer naar zulke beelden kon laten kijken. Die wordt niet moe en heeft ook geen last van psychische effecten. Wanneer ik honderdduizend uur video heb en er staat ergens een asbak op tafel, dan wil ik tegen dat systeem kunnen zeggen: waar in al dat filmmateriaal staat zo’n zelfde asbak? Of misschien is het patroon in de gordijnen hetzelfde, of is er een kerel met een tatoeage op z’n kont die vaker ergens voorkomt”, zei hij tegen Redijker. Zover was het nog niet, maar de deskundigen waar Bauwer mee samenwerkte beschouwden het als een uitdaging.

Netwerk Ook het doorzoeken van het e-mailverkeer nam nogal wat tijd in

beslag. Bauwers voorgevoel klopte: ome Jan had contact gehad met andere leden van wat op een crimineel netwerk leek. Dat was voor hen aanleiding genoeg om ook die mensen via internet in de gaten te houden. Opnieuw moest hij Redijker weerhouden van een typische beginnersfout: “Ga nooit zomaar vanaf een computer op het politiebureau internetten. Politiecomputers zitten allemaal op dezelfde server aangesloten. Zo kunnen anderen aan het ip-adres (het ‘huisnummer’ van de computer) al zien dat er rechercheurs op hun site of in hun chatroom zitten.”

Daarom hadden Bauwer en zijn collega’s een systeem opgezet waarmee elke agent anoniem onderzoek kon doen op internet. Via het systeem kregen de politiecomputers een andere identiteit, zodat ze eruit zagen als een PC met een huis-tuin-en-keuken ADSL aansluiting.

Tenslotte was er nog de mobiele telefoon van de verdachte, een stokpaardje van Bauwer: “Smartphones hebben tegenwoordig enorm veel geheugen, Redijker, waardoor er allerlei nuttige informatie op achterblijft. Niet alleen telefoonnummers, maar tegenwoordig ook foto’s.” Grinnikend vervolgde hij: “We hebben eens wat jongens opgepakt die in de wapenhandel zaten. Niemand durfde de zwijgplicht te verbreken, dus we hadden geen enkel bewijs. Maar toen we hun telefoons uitlazen, bleken ze



'Die...die plaatjes zijn daar per ongeluk op terecht gekomen, edelachtbare!'

openlijk werden verspreid via chatboxen. Ook de eerste illegale kopieerders van cd's en dvd's gingen kinderlijk simpel voor de bijl: "Op de binnenkant van de schijfjes staat een code, die aangeeft op welke stempelautomaat het schijfje gedrukt is. Zo konden we de eerste groep opsporen via het bedrijf van de stempelautomaat. Ook dat werd vervolgens tijdens de rechtszaak openbaar gemaakt, dus tegenwoordig worden die nummers vaak weggeslepen."

"Maar lopen we nog wel voorop in de digitale wapenwedloop?" vroeg Redijker.

"Jawel, tussen de negen en zes maanden, en dat is in de praktijk voldoende." De daad bij het woord voegend, lukte het Bauwer om de rond het netwerk opgetrokken anonimiteit te doorbreken en zo tientallen Europese handlangers op het spoor te komen. Dat resulteerde in arrestaties in meerdere landen, waaronder twee in Nederland.

Rechtszaak Aan het slot van de rechtszaak somde de rechter de haken en ogen van digitaal Rechercheren nog eens op: "Het moeilijkste is, om de gevonden

sporen in de juiste context te plaatsen. Bewijsbaar is wel, dat een e-mail bericht op een bepaalde computer is aangeemaakt, maar de hamvraag blijft: wie zat er op dat moment achter het toetsenbord? Jan W. woonde alleen op zijn flat en had dus als enige toegang tot de computer waarop vele illegale afbeeldingen en films met kinderporno zijn gedownload. Maar kan aangetoond worden dat de verdachte op dat moment achter de pc zat? Of dat de pc niet gehacked is? Dat kan helaas niet voor al het materiaal op zijn pc bewezen worden, alhoewel het wél zeer waarschijnlijk is dat hij zelf afbeeldingen en informatie met anderen binnen het netwerk heeft uitgewisseld.

Voor de leden van het vermeende netwerk geldt hetzelfde. Hoewel niet is aan te tonen dat de verdachten al het materiaal zelf op de computer hebben gezet, blijkt uit de tijden waarop e-mailberichten vanaf deze computer werden verstuurd met grote waarschijnlijkheid wie op welk moment aan het toetsenbord gezeten heeft. In veel gevallen achten wij dan ook deelname aan een crimineel netwerk door de verdachten bewezen. Het argument van de

advocaten, tenslotte, dat de bewuste afbeeldingen 'per ongeluk' op de pc terecht zouden zijn gekomen, maakt juridisch weinig uit, aangezien ook het in bezit hebben ervan strafbaar is."

Bauwer, die na z'n verklaring de zaak op de tribune verder gevolgd had, kende dat argument. Soms was het nog waar ook. Een gemeente wilde eens een medewerkster een officiële reprimande geven omdat de systeembeheerder pornofoto's op haar computer had aangetroffen. Pas na onderzoek door een particulier recherchebureau bleek dat die foto's daar gekomen waren omdat zij een fout had gemaakt bij het intikken van de naam van een website. Pornoboeren registreren vaak domeinnamen die veel lijken op een bekende website, met maar één of twee letters verschil.

Maar hetzelfde gold niet voor kinderporno, wist Bauwer, en dat had hij de rechters dan ook uitgelegd. Kinderpornonetwerken adverteren niet met makkelijk bereikbare websites en de kans dat iemand daar per ongeluk op terecht komt is te verwaarlozen.

"Na het afwegen van al het geleverde bewijsmateriaal, achten we de aan-

klachten voor bezit van kinderporno, ontucht en lidmaatschap van een crimineel netwerk voor Jan W. bewezen. Hij krijgt daarvoor zes jaar plus dwangverpleging opgelegd.” ■

Voor dit scenario zijn geraadpleegd: Frans Kolkman, van het interregionale bureau digitale expertise Oost-Nederland, en Matthijs van der Wel van particulier digitaal recherchebureau Fox-IT.

Zelf digitaal rechercheur worden:
www.rocasa.nl/default.asp?mid=6&id=218

Computers zijn stille getuigen van veel misdaad