Tekst: Fred Kruijer
Foto's: NFI en ANP

Gewiste beelden terughalen

Ingrijpende gebeurtenissen en strafbare feiten worden nogal eens gefilmd, door omstanders of door de daders zelf. De beelden kunnen als bewijsmateriaal dienen, mits ze niet voordien zijn gewist. Maar ook dan is nog niet alles verloren.

Van vrijwel alle belangrijke gebeurtenissen in het laatste decennium zijn particulier gemaakte videoopnamen de wereld rondgegaan. Van de aanslagen van 11 september 2001 tot en met de executie van Sadam Hoessein, het verschijnt allemaal op internet. Vrijwel altijd zijn de beelden gemaakt met particuliere camera's of telefoons. En ook een winkeloverval of geweldsincident is nogal eens gefilmd door omstanders, of door de daders zelf. Dit soort opnamen spelen steeds vaker een rol als bewijsmateriaal in een eventuele rechtszaak. Maar na het opslaan van de gefilmde beelden op gegevensdragers - zoals de al dan niet losse opslagkaart van de telefoon of de harde schijf van de computer - worden opgenomen beelden soms al dan niet per ongeluk gewist. Het goede nieuws is dat gewiste videobeelden vaak toch nog te herstellen zijn. Dat kon al eerder, maar nu zijn de mogelijkheden aanzienlijk toegenomen met het softwareprogramma Defraser, ontwikkeld door het Nederlands Forensisch Instituut (NFI).

Manipulatie

Voor alle duidelijkheid: Defraser is geen software om beelden te verscherpen, verbeteren of verduidelijken. In een eerder in Blauw geplaatst bericht over Defraser stond een onduidelijke foto met een vage grijze stip, met daarnaast het 'verbeterde' plaatje met een scherp omlijnde straaljager. Dat is echter niet wat Defraser doet. Een vage digitale foto betekent dat de lens niet scherp stond toen hij genomen werd, dat de beeldresolutie te laag is of dat het beeld bij opslag te sterk gecomprimeerd is waardoor informatie verloren is gegaan. Ook een vuile of natte lens kan een oorzaak zijn. Maar om foto's te verscherpen die van zichzelf niet scherp zijn, moet de computer pixels verzinnen die er eenvoudig niet zijn. Zeno Geradts is forensisch onderzoeker van de groep Beeldonderzoek en Biometrie van de afdeling Digitale Technologie en Biometrie van het NFI. "Als je beelden gaat verscherpen, begin je al met de kleurwaarde van pixels aan te tasten. Voeg je iets toe of verander je iets, dan ben je in wezen iets aan het verzinnen. Dat zou manipulatie van het materiaal zijn. Daar

Enkele nieuwe mogelijkheden

- Defraser kan een thumbnailoverzicht genereren van alle op een gegevensdrager gevonden videobestandsfragmenten. Dat geeft snel inzicht in de beeldinhoud van een gegevensdrager. Dit is een relatief recente toevoeging aan Defraser, die erg veel tijd kan schelen in een onderzoek.
- In sommige gevallen kunnen juist die metadata overschreven zijn die benodigd zijn voor het weergeven van de beelddata in een gevonden videobestandsfragment (denk aan de beeldresolutie, of de naam van het gebruikte codec). Defraser biedt echter de mogelijkheid de beelden alsnog te kunnen weergeven door de missende metadata uit een wèl werkend videobestand te gebruiken. Dit kan handmatig in Defraser, waarbij bestandsonderdelen als een soort puzzel gecombineerd kunnen worden. Daarvoor is kennis van de opbouw van videobestanden wel handig. Defraser kan het echter in bepaalde gevallen ook automatisch. Hiertoe dient dan een goed afspeelbaar videobestand ingesteld te worden als referentie, waarna Defraser automatisch de missende metadata opzoekt en gebruikt voor de weergave van de beelden.

houden wij ons bij het NFI niet mee bezig."

Wissen

Defraser is dan ook beter te omschrijven als een programma dat het mogelijk maakt om gewiste videobeelden in sommige gevallen geheel of gedeeltelijk te herstellen. Rikkert Zoun, forensisch onderzoeker bij de groep Beeldonderzoek en Biometrie legt uit op welke wijze videobeelden op een gegevensdrager worden bewaard. "Een gegevensdrager heeft over het algemeen een bestandssysteem, een soort bestandsadministratie. Een gedeelte van de opslagruimte op de gegevensdrager is gereserveerd voor tabellen die aangeven op welke plek op de gegevensdrager de bestandsdata te vinden zijn. Een besturingssysteem, zoals Windows, maakt gebruik van de informatie in dat bestandssysteem om de betreffende bestanden te kunnen benaderen. Sla je een videobestand op op een gegevensdrager, dan wordt voor dat bestand een entry aangemaakt in de tabellen in het bestandssysteem. Om het bestand te kunnen afspelen, kan Windows via die tabel onder meer de juiste bestandsplaatsen vinden om het bestand vervolgens via een player af te spelen." Handig, want de bestandsdelen worden vaak op verschillende plaatsen op de gegevensdrager weggeschreven, namelijk waar nog ruimte is op de schijf.
Wordt het bestand – al dan niet per ongeluk – gewist, dan verandert er in eerste instantie alleen iets in de tabelinformatie. Het bestand is dan voor Windows niet meer zo eenvoudig benaderbaar. Bovendien komt de bestandsruimte waarop de beelden stonden weer vrij om opnieuw te overschrijven. Zolang dat laatste niet gebeurt, is de gewiste informatie met de juiste software alsnog te herstellen en toegankelijk te maken. Defraser kan dat. Sterker nog, de kracht van het programma is dat het ook fragmenten van bestanden kan detecteren. Is een deel van het bestand dus al weer overschreven, dan gaat Defraser op zoek naar wat er nog aan bruikbare informatie over is en maakt deze opnieuw toegankelijk.
Bij het opslaan van een videobestand worden, naast de daadwerkelijke beelden, ook zogenaamde metadata opgeslagen in het bestand. Een voorbeeld daarvan is het zogenaamde tijdstempel, waaruit blijkt wanneer het filmpje is aangemaakt - vooropgesteld dat de cameratijd correct was ingesteld. Ook deze data zijn op dezelfde wijze terug te halen en dat is mooi, want dit soort gegevens kunnen mede als bewijs dienen.

Comprimeren

Defraser werkt niet automatisch voor alle videoformats. Een videobeeld bestaat altijd uit een aantal pixels die samen een beeld op een scherm tonen, maar de manier waarop beelden worden opgeslagen op gegevensdragers verschilt. Uit de bestandsextensie en de metadata in een videobestand is meestal af te leiden op welke wijze de beelden zijn opgeslagen. Hierbij wordt vaak verwezen naar de 'codec', een samenvoeging van de woorden encoder en decoder. Dat betekent het comprimeren en decomprimeren van beelden. Beelden nemen veel ruimte in op een gegevensdrager. Maar videobeelden zijn tegenwoordig eenvoudig te comprimeren. Soms gebeurt dat door details of kleine kleurverschillen tussen naburige pixels uit te vlakken die relatief weinig invloed hebben op de visuele kwaliteit van een beeld. Daarnaast kan ook ruimte bespaard worden door herhalende patronen op een slimme manier op te slaan. Een eenvoudig voorbeeld hiervan is dat duizend dezelfde bytes ook kunnen worden omschreven met het commando: 'Plaats hier duizend dezelfde bytes.' Het eindresultaat van compressie van videobeelden is in de meeste gevallen wel dat de beeldkwaliteit er op achteruit gaat.

Steeds vaker worden gebeurtenissen gefilmd door omstanders. Gewiste beelden zijn in sommige gevallen nog terug te halen met speciale software.

>>

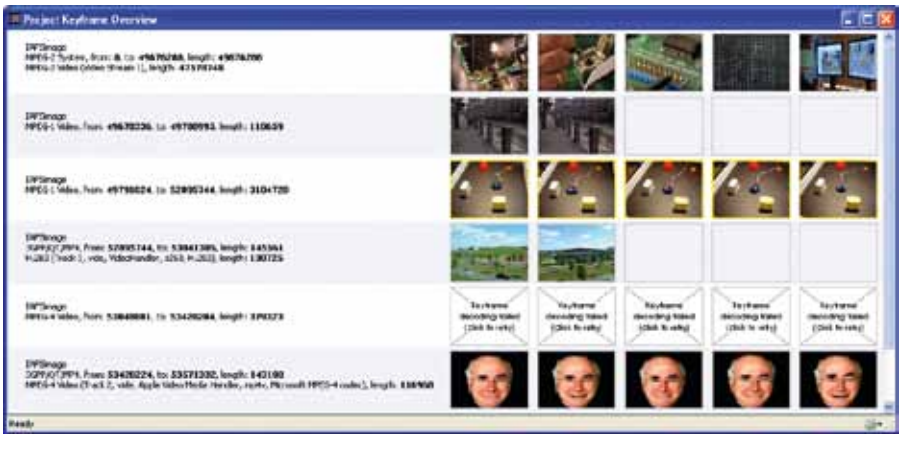
>> Iedere codec doet dat comprimeren anders. En de technieken om zoveel mogelijk informatie zo efficiënt mogelijk weg te schrijven, verbeteren nog altijd en leiden steeds weer tot nieuwe videoformats. Defraser is dus doorlopend in ontwikkeling en de gebruikers zijn daarbij betrokken via een klankbordgroep. Voortdurend worden nieuwe stukjes software – plug-ins - toegevoegd aan Defraser, waarmee beelden kunnen worden hersteld die met nieuwe codecs zijn weggeschreven. Beschikbare plug-ins zijn AVI, 3GP/MP4/QuickTime, MPEG 1,2 en 4, H.263, ASF/WMV. Het NFI werkt op dit moment aan de ontwikkeling van andere formats. Dat kost geld. In het kader van het Programma Aanpak Cybercrime loopt een aanvraag via politie Haaglanden bij VtsPN, om het nieuwe format H.264 toegankelijk te maken voor Defraser.

Integriteit

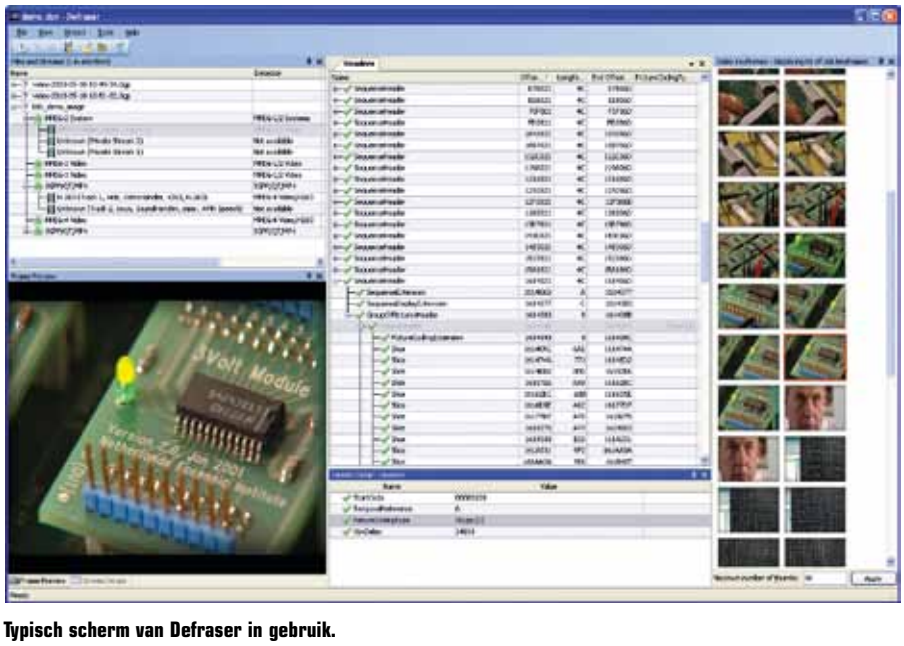
Tot voor kort moest de politie gegevensdragers met gewiste informatie inleveren bij het NFI, maar daar ontdekte men al snel dat het vaak om dezelfde videoformats ging. Reden voor Rikkert Zoun en Zeno Geradts om de software zodanig te ontwikkelen dat rechercheurs zonder tussenkomst van het NFI zelf videobeelden op gegevensdragers kunnen terugvinden en herstellen. Waar nodig beschikt het NFI nog altijd over kennis om te helpen indien ook Defraser geen afdoende oplossing biedt. Defraser kent ook al de nodige buitenlandse gebruikers. Het NFI is lid van het European Network of Forensic Science Institutes. Het programma wordt al gebruikt in onder meer Duitsland en Zweden. Maar de software is algemeen beschikbaar en eigenlijk iedereen kan het downloaden. Dat doet geen afbreuk aan de integriteit van de onderzoeksresultaten van Defraser. Zoun: "Defraser voegt geen beelddata of pixels toe. Als je met Defraser beelden terugvindt en weergeeft, gaat het altijd om originele teruggevonden beelden op de gegevensdrager die je weer kunt gebruiken."

Versterken

"Als digitaal rechercheur vind ik het programma Defraser een zeer nuttige tool," zegt Jos van den Oetelaar van de afdeling Digitale Recherche van de Bovenregionale Recherche Zuid-Nederland. "Wij maken veel gebruik van forensische programma's als EnCase en FTK. Die kunnen echter over het algemeen alleen maar gewiste AVI-bestanden terughalen en dan nog alleen als de header van het bestand wordt aangetroffen. Defraser haalt fragmenten van veel meer videoformats terug, zonder dat daarvoor een header nodig is. Het programma vindt dus ook videofragmenten terug die al deels weer overschreven zijn en kan daarvan de delen die niet zijn overschreven vaak weer herstellen. Deze fragmenten kunnen soms net genoeg zijn om je zaak te versterken dan wel in de goede richting te zetten." ■



Voorbeeld van het 'thumbnailoverzicht', dat snel overzicht geeft van de op de gegevensdrager aangetroffen videobestandsfragmenten.



Typisch scherm van Defraser in gebruik.

Defraser hoeft niet te worden besteld. Het programma is eenvoudig te downloaden op http://sourceforge.net/projects/defraser.

Fred.kruijer@politieacademie.nl

Voor meer informatie:

PKN > Forensische opsporing > Digitale opsporing > Computeronderzoek

PKN > Forensische opsporing > Digitale opsporing > Mobiele telefoononderzoek

PKN > Forensische opsporing > Digitale opsporing > Onderzoek aan digitale elektronica