Inhoudsopgave

1. De vakbijlage algemeen

Sinds oktober 2015 biedt het Nederlands Forensisch Instituut (NFI) in samenwerking met de opsporingsdiensten de dienst Hansken aan. Deze dienst ondersteunt het doorzoeken van (inbeslaggenomen) digitaal materiaal. Deze vakbijlage is ontwikkeld om als naslagwerk te dienen in een procesdossier. Deze vakbijlage dient als toelichting op de dienst en heeft een zuiver informatief karakter. De vakbijlage geeft weer hoe een onderzoek met behulp van Hansken in het algemeen plaatsvindt en welke aandachtspunten er bij een dergelijk onderzoek zijn. Aan het einde van de vakbijlage zijn een verklarende woordenlijst en een algemene literatuurverwijzing opgenomen.

2. Inleiding

De hoeveelheid te onderzoeken gegevens en gegevensbronnen in strafzaken neemt razendsnel toe. Om de effectiviteit en snelheid van dit onderzoek te vergroten, heeft het Nederlands Forensisch Instituut (NFI) de

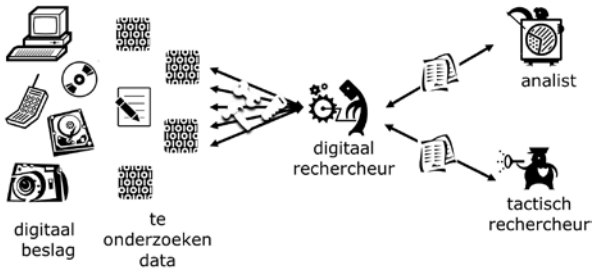
forensische dienst Hansken ontwikkeld. Het doel van Hansken is om de juiste personen, op het juiste moment, toegang te geven tot de juiste informatie.

Met Hansken kan een onderzoeksteam snel en efficiënt zoeken in grote hoeveelheden in beslaggenomen gegevensdragers als computers en mobiele telefoons. Op alles wat relevant kan zijn, kan worden gezocht, bijvoorbeeld op woorden en namen of eigenschappen van *sporen* zoals chatberichten, e-mails of foto's al dan niet gemaakt met een bepaalde camera.

Rechercheurs kunnen met de forensische dienst de zoekresultaten blijven filteren totdat je van die miljoenen sporen een selectie hebt, waarvan de sporen één voor één te bekijken zijn.

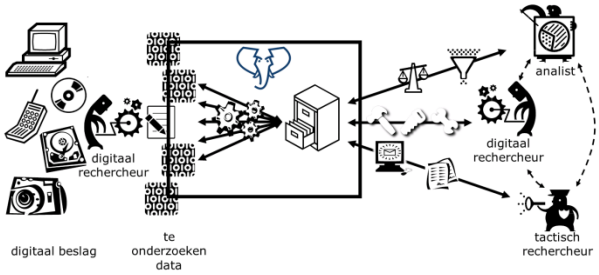
3. Beschrijving van het proces

Hansken biedt een alternatief voor het traditionele proces voor digitaal forensisch onderzoek.



Figuur 1 Het traditionele proces voor het digitaal forensisch onderzoek

Figuur 1 geeft het proces weer zonder dat gebruik wordt gemaakt van Hansken. Hierbij is de digitaal rechercheur de persoon die het onderzoek uitvoert en hierover rapporteert aan degene die vragen heeft over het bewijsmateriaal (digitaal beslag).



Figuur 2 Het proces voor het digitaal forensisch onderzoek met gebruik van Hansken

Figuur 2 toont het proces waarbij gebruik wordt gemaakt van Hansken. Hierbij is de digitaal rechercheur niet langer de centrale deelnemer maar kan de vraagsteller (tactisch rechercheur of analist) zelf in het digitaal bewijsmateriaal zoeken. Bij aanvullende vragen of de behoefte tot nadere duiding kan de digitaal rechercheur worden ingeschakeld.

3.1. Veiligstellen

Zoals bij elk digitaal forensisch onderzoek wordt begonnen met het maken van één-op-één-kopieën of een logische extractie van digitale bewijsmiddelen zoals van een harde schijf of een mobiele telefoon. Het veiligstellen gebeurt door de opdrachtgever volgens de hiervoor geldende procedures.

3.2. Verwerking van de gegevens

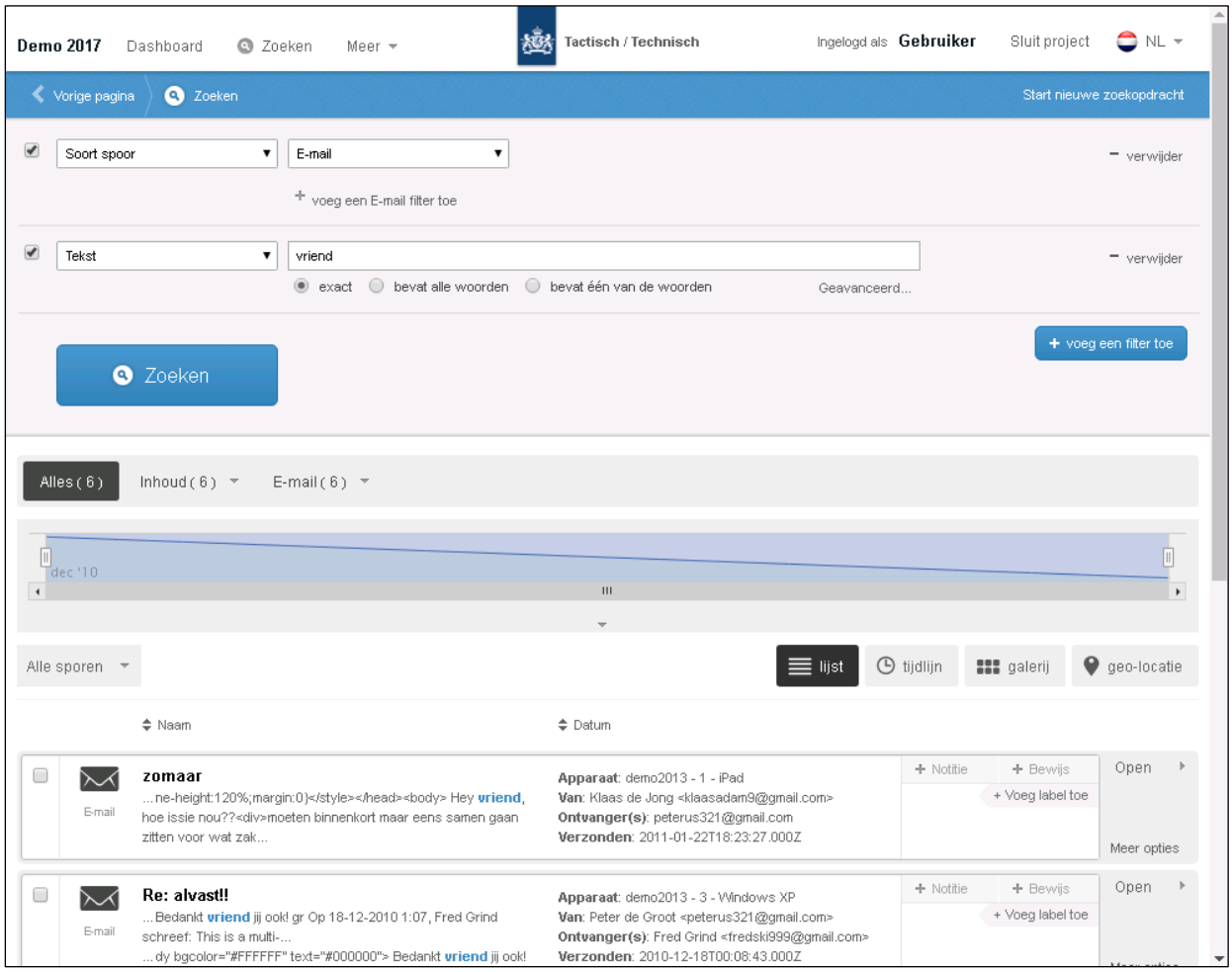
Bij de aanvraag van een Hansken-zaak levert de opdrachtgever informatie aan over een zaak, zoals de naamgeving en wie toegang mag krijgen tot de gegevens.

De bij de zaak behorende veiliggestelde gegevens (bewijsbestanden) worden door de opdrachtgever naar Hansken geüpload of aangeleverd bij het NFI en door het NFI geüpload. Het is mogelijk om deze gegevens te voorzien van aanvullende (tactische) informatie, zoals de locatie waarop en/of persoon bij wie de gegevens zijn aangetroffen. Deze informatie wordt in Hansken bij de bewijsbestanden vastgelegd en kan later gebruikt worden bij het zoeken.

In Hansken worden bewijsbestanden (per zaak) samengevoegd in een *project*.

Vervolgens maakt Hansken structuren inzichtelijk die per project in één index worden vastgelegd. Per bewijsbestand vindt een extractie plaats waarbij herkenbare digitale objecten, ook wel *sporen* genoemd, uit het bewijsbestand worden gehaald. Voorbeelden zijn e-mails, chatgesprekken, PDF-documenten en digitale afbeeldingen.

Tijdens de extractie wordt een basisverzameling aan *tools* toegepast om zoveel mogelijk sporen uit de bewijsbestanden te halen. Enkele voorbeelden van dergelijke tools zijn tools die bestanden en mappen uit *bestandssystemen* halen, tools die logische rapportages van andere tools zoals UFED en XRY uitlezen, tools die e-mails en contactpersonen uit e-maildatabases lezen, tools die tekst uit afbeeldingen kunnen halen met *OCR* en tools die verwijderde bestanden kunnen terughalen. Deze verzameling kan op aanvraag uitgebreid worden met enkele specialistische tools. Op aanvraag verstrekt het NFI een overzicht van de beschikbare tools.



Figuur 3 voorbeeld van de tactische gebruikersinterface van Hansken

Wereldwijd wordt een grote diversiteit aan soft- en hardware gebruikt, wat zorgt voor een grote verscheidenheid aan sporen. Bij sporen van hetzelfde type kunnen verschillende eigenschappen worden opgeslagen. De eigenschappen die bij een e-mailbericht behoren zijn bijvoorbeeld anders als dit bericht wordt opgeslagen door Microsoft Office Outlook dan wanneer dit gebeurt door de standaard mailapplicatie op een iPhone.

De *tools* in Hansken vertalen deze verschillende vormen van sporen naar het uniforme datamodel voor Hansken, zodat deze later makkelijker doorzocht kunnen worden.

3.3. Doorzoeken van sporen

De sporen kunnen door een rechercheur, analist, forensisch onderzoeker of een andere belanghebbende worden doorzocht. Om een zoekvraag te stellen, wordt gebruik gemaakt van een specifiek voor Hansken ontwikkelde zoektaal. Deze zoektaal, de *Hansken Query Language*, is gebaseerd op een bestaande zoektaal, de *Lucene Query Language*.

Om de eindgebruikers te ondersteunen, zijn in samenwerking met eindgebruikers meerdere gebruikersinterfaces (*grafische user interfaces*) ontwikkeld. De twee belangrijkste zijn de tactische en de technische gebruikersinterface.

De tactische gebruikersinterface, gericht op tactisch rechercheurs, heeft als doel om informatie zo herkenbaar mogelijk te presenteren en om het zoeken eenvoudig te maken. Voor het gebruik van deze interface is dan ook de geen digitaal expertise nodig. Figuur 3 toont een voorbeeld van de tactische gebruikersinterface.

De technische gebruikersinterface geeft de rechercheur alle beschikbare informatie en biedt uitgebreide zoek- en presentatiemogelijkheden. De doelgroep van deze

gebruikersinterface is de rechercheur die meer affiniteit heeft met digitaal forensisch onderzoek.
Zoeken met Hansken gebeurt door filters toe te passen op de sporen. Als geen filter wordt toegepast, worden *alle* sporen binnen het geopende project weergegeven. Hierbij is het mogelijk om sporen individueel te bekijken. Als de gebruiker een filter instelt, blijft het aantal sporen gelijk of wordt kleiner. Hierdoor is het mogelijk om snel en efficiënt in te zoomen op de revelante sporen. De ingestelde filters kunnen ook worden verwijderd of aangepast indien dit nodig is.

Voorbeelden van filters zijn zoekwoorden, datum- en tijdinformatie en eigenschappen van sporen (*metadata*), zoals de afzender van een e-mailbericht. Doordat binnen Hansken gebruik wordt gemaakt van een datamodel, kunnen deze filters op een uniforme manier worden ingesteld.

Bij het zoeken op woorden kan worden aangeven waar woorden moeten voorkomen en hoe woorden gecombineerd moeten worden. Er kan in de inhoud van sporen, in eigenschappen (metadata) of in beide gezocht worden. Daarnaast kan worden aangegeven of minstens één woord of alle woorden moeten voorkomen en of ze wel of niet in de opgegeven volgorde moeten staan. Ook op delen van woorden kan worden gezocht. Hansken is niet gevoelig voor hoofdletters of bijzondere leestekens. Woorden korter dan drie letters worden niet meegenomen.

De sporen in het zoekresultaat kunnen worden gesorteerd op relevantie met betrekking tot de zoekvraag[1], datum en tijd of specifieke eigenschappen van de sporen.

4. Functionaliteit

Hansken biedt functionaliteit die specifiek is ontwikkeld om het onderzoeksproces te ondersteunen. In deze sectie wordt een aantal functionaliteiten nader beschreven.

4.1. Labels en notities

Als gedurende een onderzoek een spoor wordt gevonden waarbij de wens staat deze te markeren, is dit op twee manieren mogelijk. Ten eerste kan een label aan een spoor of set aan sporen worden toegekend. Labels zijn korte beschrijvingen van één of een aantal woorden waarbij verder geen informatie over bijvoorbeeld de auteur wordt vastgelegd. Met deze labels kunnen sporen worden gegroepeerd. Ten tweede kan een notitie aan een spoor worden toegevoegd. Hierbij kan meer informatie worden geplaatst en worden de auteur en het tijdstip bijgehouden. Voor zowel labels als notities geldt dat er meer dan één aan een spoor kan worden gekoppeld.

4.2. Rapportage

Indien een spoor wordt aangetroffen waarvan het nuttig is de eigenschappen te rapporteren, is het mogelijk om een rapportage vanuit Hansken te genereren. Zo'n rapport bevat een feitelijke weergave van het spoor, d.w.z. de aangetroffen structuur die leidt tot het spoor én de aangetroffen metadata van het spoor zelf. Naast de eigenschappen van het spoor is het mogelijk om andere informatie op te nemen, zoals de notities en labels, de inhoud van het spoor en de versie van Hansken en de gebruikte tools.

De versie van Hansken en de gebruikte tools geven informatie over de plaats waarop het spoor in het bewijsbestand is aangetroffen. Dit is van belang voor de *chain of evidence*. Vanwege het continu verbeteren van de software is het mogelijk dat in latere versies van Hansken of van de tools andere of nieuwe sporen geïdentificeerd worden.

4.3. Sporenverzameling

Tijdens de extractie ontstaat een sporenverzameling met alle sporen uit het digitaal beslag. Soms bevat deze volledige sporenverzamelingsporen die niet ingezien mogen worden door een gebruiker, bijvoorbeeld vanwege de proportionaliteit van het onderzoek aan deze sporen. Hansken kan de volledige sporenverzameling reduceren tot een sporenverzameling met een klein deel van de sporen. De gereduceerdesporenverzameling wordt gekoppeld aan een project, hierdoor krijgen de gebruikers geen inzicht in de volledige set van sporen.

In essentie houdt de functionaliteit in dat het mogelijk is om vooraf een lijst van woorden op te geven waarbij na verwerking van deze lijst alleen sporen met voorkomens van een of meerdere woorden worden getoond aan gebruikers.

4.4. Geheimhouderscommunicatie

Onder geheimhouderscommunicatie wordt verstaan communicatie tussen de verdachte en een verschoningsgerechtigde zoals een arts of advocaat. Deze communicatie mag niet gebruikt worden in het onderzoek. Hansken bevat daarom functionaliteit om dergelijke sporen uit te sluiten van het onderzoek. De functionaliteit sluit aan op de werkwijze beschreven in de "Handleiding Verwerking

[1] Relevantie wordt bepaald op basis van de tf/idf-score (term frequency inverse document frequency) van een spoor: de verhouding van de voorkomens van het woord in een spoor ten opzichte van de grootte van het spoor en de voorkomens van het woord in de volledige index van de zaak.

geheimhouderinformatie aangetroffen in inbeslaggenomen voorwerpen en in digitale bestanden" van de Landelijke Vergadering Rechercheofficieren juni 2014.

In essentie houdt de functionaliteit in dat het mogelijk is om vooraf een lijst van woorden op te geven waarbij na verwerking van deze lijst alle sporen met voorkomens van een of meerdere woorden niet worden getoond aan gebruikers. In enkele gevallen is mogelijk dat sporen ten onrechte niet worden herkend als geheim en dus niet worden gemarkeerd. Daarom is het ook mogelijk dat een rechercheur gedurende het onderzoek sporen aanmerkt als vertrouwelijk. Hierbij wordt het spoor direct verwijderd uit de zoekresultaten.

Omdat het ook mogelijk is dat iets onterecht als geheimhouderscommunicatie wordt aangemerkt, kan een persoon worden aangewezen als "medewerker geheimhouders". Deze persoon heeft de rechten om geheimhouderscommunicatie in te zien en deze status van een spoor af te halen zodat het spoor weer in te zien is door rechercheurs.

4.5. Eigen sporen toevoegen

Het is mogelijk dat gebruikers zelf met tools buiten Hansken om sporen uit gegevens afleiden. Ook zulke sporen kunnen aan Hansken toegevoegd worden. Het datamodel van Hansken ondersteunt dit door onderscheid te maken tussen sporen toegevoegd door de Hansken *tools* en sporen toegevoegd door gebruiker*stools*. Bij deze functionaliteit wordt ook de *chain of evidence* bewaakt doordat geadministreerd wordt wie wanneer welke sporen toevoegt.

5. Rolverdeling en verantwoordelijkheden

Het NFI heeft Hansken ontwikkeld in samenwerking met onder andere de Nationale Politie en de FIOD. Om de kwaliteit van zowel het onderzoeksproces als de dienst Hansken te garanderen, zijn er afspraken gemaakt over verantwoordelijkheden, opleiding, bevoegdheden en kwaliteit.

5.1. Verantwoordelijkheden

De medewerkers van de opsporingsdiensten doen zelfstandig onderzoek met Hansken en zijn zelf verantwoordelijk voor de vastligging van de onderzoeksresultaten.

Het NFI is verantwoordelijk voor de programmacode van Hansken.

De Nationale Politie en de FIOD beheren zelf een eigen implementatie van Hansken inclusief de onderliggende infrastructuur, dat wil zeggen de hardware waar Hansken op draait en de benodigde systeemsoftware. Het NFI ondersteunt de Nationale Politie met applicatiebeheer, zoals het aanmaken van projecten en het verwerken van bewijsbestanden. Op dit moment kan een aantal politie-eenheden zelf bewijsbestanden in Hansken plaatsen. De bedoeling is dat dit op termijn vanuit alle politie-eenheden mogelijk is.

Voor andere organisaties (inclusief het NFI) ligt de volledige verantwoordelijkheid voor de dienst bij het NFI.

De wensen voor nieuwe functionaliteiten komen bij de gebruikers vandaan en de verantwoordelijkheid voor het inplannen van deze wensen ligt bij het ontwikkelteam van het NFI. Het gebeurt regelmatig dat een specifiek onderzoek om specifieke functionaliteit vraagt. Het uitgangspunt van het NFI bij toevoegen van deze functionaliteit is dat het altijd dusdanig generiek dient te zijn dat het ook voor andere onderzoeken toegevoegde waarde heeft.

5.2. Gebruikersrechten

Het rechtenmodel van Hansken is ingericht volgens het *Role-based access control*-model. In essentie komt dit model er op neer dat een gebruiker alleen iets mag, indien hij hier expliciet toestemming voor heeft. Voorbeelden van rechten zijn het mogen aanmaken van projecten, het mogen toevoegen van labels en het mogen inzien van geheimhouderscommunicatie. Door deze manier van toegang verlenen, is het niet mogelijk om een functie uit te voeren waarvoor de gebruiker geen toestemming heeft. Het toekennen van deze toestemming gebeurt door de applicatiebeheerder van Hansken.

5.3. Sleutelbeheer

Gegevens in Hansken worden versleuteld opgeslagen. Om deze gegevens te ontsleutelen, is een digitale sleutel nodig. Deze sleutel wordt opgeslagen buiten Hansken en moet worden aangeleverd bij het ophalen van gegevens. Het is voor beheerders van de omgeving (zonder toegang tot de sleutels) dan ook niet mogelijk om deze gegevens in te zien. Iemand die toegang heeft tot een sleutel, kan deze sleutel met andere gebruikers delen.

6. Kwaliteitsmaatregelen

Om de kwaliteit van de dienst en de daaruit voortvloeiende resultaten te waarborgen, is een aantal maatregelen genomen.

6.1. Opleiding en bevoegdheden

Voordat een gebruiker de dienst gebruikt, wordt sterk aangeraden de gebruiker een Hansken-training te laten volgen. Deze trainingen worden verzorgd door het NFI en de Politieacademie. Tijdens deze training krijgt de gebruiker inzicht in het digitaal forensisch onderzoek en digitale sporen. Ook gaat de gebruiker werken met Hansken, bij voorkeur in een operationele zaak.

Gebruikers die toestemming hebben om gegevens (bewijsbestanden) in Hansken te plaatsen, krijgen een gerichte instructie om zorg te dragen dat de infrastructuur van Hansken niet overbelast raakt.

6.2. Softwareontwikkeling

Het ontwikkelproces is zo ingericht dat bij elke wijziging van de Hansken-programmacode door een ontwikkelaar tenminste twee andere ontwikkelaars akkoord op de wijziging dienen te geven. Onderdeel van de *best practices* bij codeontwikkeling is dat de wijzigingen worden ondersteund door bijbehorende tests die de functionaliteit aantoont.

6.3. Tests

Voordat een codewijziging wordt geaccepteerd, dienen alle aanwezige tests te slagen. Iedere test, een zogenaamde *unit test*, toont aan dat één specifiek onderdeel van Hansken naar verwachting functioneert.

Voordat een nieuwe versie van Hansken wordt vrijgegeven voor productie, wordt naast de losse onderdelen ook de correcte werking van de gehele dienst getest. Hierbij wordt de dienst Hansken opgestart in een omgeving die vergelijkbaar is met de productieomgeving. Vervolgens worden zogenaamde *integratietests* uitgevoerd die de dienst testen. Hierbij geldt dat één falende test er voor zorgt dat een onderzoek naar de oorzaak wordt ingesteld en de nieuwe versie niet wordt vrijgegeven voor productie.

6.4. Controle van de resultaten

Hoewel bij het testen over het algemeen de belangrijkste fouten worden achterhaald, is het niet ondenkbaar dat in productie toch fouten optreden. Hierbij zijn twee soorten fouten te onderscheiden: resultaten kunnen onvolledig zijn en resultaten kunnen incorrect zijn. Na een extractie wordt door de operationeel beheerders een aantal standaardresultaten bekeken om te bepalen of de extractie naar verwachting is verlopen. Bij een onverwachte afwijking wordt onderzoek ingesteld naar de oorzaak en wordt de opdrachtgever geïnformeerd over de afwijking.

Gebruikers worden er, bijvoorbeeld tijdens de opleiding, op gewezen dat resultaten die van belang zijn voor het onderzoek altijd dienen te worden gecontroleerd met andere software. Hiervoor kunnen zij zich wenden tot een digitaal rechercheur. Dit is ook verstandig indien onduidelijkheid bestaat over de resultaten. Het NFI schrijft niet voor hoe over sporen moet worden geverbaliseerd, aangeraden wordt om dit zo veel mogelijk in samenwerking met een digitaal rechercheur te doen.

7. Verklarende woordenlijst

Best practice Een in de praktijk toegepaste techniek, methode of manier van werken die aantoonbaar zeer goed functioneert.

Chain of evidence De chain of evidence legt zo gedetailleerd mogelijk vast wat er met onderzoeksmateriaal is gebeurd en/of hoe het tot stand is gekomen, vanaf het eerste moment waarop het onderdeel werd van een onderzoek.

Sporenverzameling Een verzameling van sporen uit digitaal beslag. De volledige sporenverzameling zijn alle sporen na extractie, een deel sporenverzameling is een selectie uit de volledige sporenverzameling.

Metadata Data over data, bijvoorbeeld de naam van een bestand, de afzender van een e-mailbericht of het merk camera waarmee een digitale foto is gemaakt.

OCR Optical Character Recognition (OCR), in het Nederlands optische tekenherkenning, is een techniek waarbij uit een digitale afbeelding door middel van patroonherkenning tekst wordt gehaald.

Project Een met Hansken doorzoekbare verzameling gegevens (bewijsbestanden), in de praktijk vaak overeenkomend met de gegevens binnen één (straf)zaak.

Role-based access control Toegangscontrole, waarbij rechten worden gekoppeld aan rollen binnen een organisatie of bedrijfsproces. Individuen verkrijgen de rechten door een bepaalde rol te vervullen.

Sporen Voor gebruikers herkenbare digitale objecten, bijvoorbeeld e-mails, chatberichten, digitale afbeeldingen, opgemaakte tekstdocumenten en spreadsheets.

Tools Gereedschappen die tijdens de extractie gebruikt worden voor de analyse van specifieke digitale sporen met als doel deze sporen te verrijken en/of nieuwe sporen uit deze sporen te extraheren. Een overzicht van de beschikbare tools is op te vragen bij het NFI.

8. Literatuur

In de vakbijlage zijn geen expliciete verwijzingen gebruikt naar literatuur, aangezien het eigen ontwikkelde

programmatuur betreft. Over het veranderende proces en de manier hoe dit in Hansken is vormgegeven zijn twee publicaties geschreven die goed als referentie te gebruiken zijn:

1. Van Baar, R. B., Van Beek, H. M. A. en Van Eijk, E. J. "Digital Forensics as a Service: A game changer." *Digital Investigation 11* (2014): S54-S62.2, beschikbaar op https://doi.org/10.1016/j.diin.2014.03.007
2. Van Beek, H. M. A., et al. "Digital forensics as a Service: Game on." *Digital Investigation 15* (2015): 20-38, beschikbaar op https://doi.org/10.1016/j.diin.2015.07.004

Voor algemene vragen kunt u contact opnemen met de Frontdesk, telefoon (070) 888 68 88. Voor inhoudelijke vragen kunt u contact opnemen met de divisie Digitale en Biometrische Sporen telefoon (070) 888 64 00.

Nederlands Forensisch Instituut
Ministerie van Justitie en Veiligheid
Postbus 24044 | 2490 AA Den Haag

Telefoon (070) 888 66 66
www.forensischinstituut.nl