Nederlands Forensisch Instituut
Ministerie van Justitie en Veiligheid

Informatieblad

Forensische waarborgen in Hansken

Inhoudsopgave

1. 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) het forensisch platform Hansken ontwikkeld.

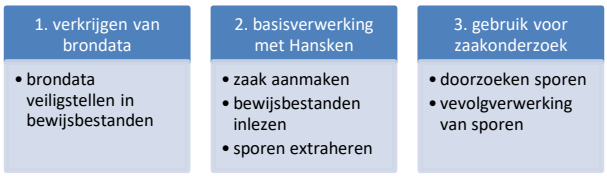
Het doel van Hansken is informatie uit digitale stukken van overtuiging zoals telefoons en computers snel en laagdrempelig inzichtelijk te maken voor gebruikers (met of zonder specifieke IT-kennis) die geautoriseerd zijn voor onderzoek aan deze stukken van overtuiging. Dit doet Hansken door de gegevens te structureren en indexeren. Op alles wat relevant kan zijn, kan vervolgens worden gezocht, bijvoorbeeld op woorden en namen of eigenschappen van *digitale sporen* zoals bestanden, chatberichten, e-mails of foto's al dan niet gemaakt met een bepaalde camera.

Een gebruiker kan met Hansken de zoekresultaten blijven filteren totdat van die miljoenen sporen een beheersbare selectie overblijft, waarvan de sporen één voor één te bekijken zijn.

Algemene informatie en uitleg over Hansken is beschikbaar in de *Vakbijlage Hansken*[1].

In steeds meer strafzaken worden met Hansken gevonden sporen als bewijs gebruikt. Dit vereist gedegen forensische onderbouwing: het materiaal moet op een transparante manier verwerkt worden en de gerapporteerde sporen moeten herleidbaar zijn naar de bron (bijv. de inbeslaggenomen telefoon of computer).

De inzet van Hansken bevat meerdere waarborgen ten behoeve van deze onderbouwing. Dit informatieblad licht deze waarborgen toe aan de hand van de stappen in het onderzoeksproces:



Hierbij wordt onderscheid gemaakt in de verwerking van het bewijsmateriaal[2] zelf (chain of evidence) en vastlegging van het verwerkingsproces (chain of custody).

Voor de vastlegging van gebruikershandelingen biedt Hansken de mogelijkheid om auditinformatie naar een auditsysteem te sturen. Deze functie stuurt informatie over alle verzoeken aan Hansken door, inclusief de datum en tijd, gebruiker en details van het desbetreffende verzoek.

1.1. Hansken onderzoeksomgevingen

Opsporingsdiensten beschikken in principe over een eigen Hansken-omgeving in hun eigen datacentra. Sommige opsporingsdiensten maken gebruik van verschillende Hansken-omgevingen van het NFI of van andere organisaties. Het NFI biedt ook een gescheiden Hansken-omgeving aan voor de inzage in specifiek bewijsmateriaal door advocaten en de rechtelijke macht.[3]

Medewerkers van de eigen organisatie beheren hun eigen Hansken-omgeving. Hierbij wordt onderscheid gemaakt tussen systeembeheerders (infrastructuur, hardware, onderliggende software en Hansken platform) en functioneel beheerders (inzet van Hansken voor specifiek zaakonderzoek).

Enkele functioneel beheerders van de Hansken-omgeving bij de Nationale Politie voeren de handelingen (in opdracht van de Nationale Politie) uit vanuit het NFI. Deze beheerders beheren ook de NFI-omgevingen (in opdracht van het NFI).

2. Verkrijgen van brondata

De brondata is de dataverzameling die uit de inbeslaggenomen apparaten is veiliggesteld of is gevorderd bij bijvoorbeeld providers.

2.1. Brondata veiligstellen

Het veiligstellen van deze brondata vindt plaats in bewijsbestanden, ook wel images genoemd. Zo'n bewijsbestand bevat naast de veiliggestelde brondata vaak ook gegevens over het veiligstellen, zoals informatie over het veiliggestelde apparaat, het tijdstip van veiligstellen en de betrokken personen.

Om de integriteit van brondata te borgen, worden bij het veiligstellen bestandskenmerken[4] van de brondata berekend, ook wel hashes of digests genoemd. Deze bestandkenmerken zijn reproduceerbaar en worden vaak ook in het bewijsbestand vastgelegd.

Dit veiligstellen gebeurt door medewerkers van de opsporingsdiensten en staat los van (het gebruik van) Hansken.

2.1.1. Verwerking van het bewijsmateriaal

Een bewijsbestand wordt tijdens een onderzoek normaalgesproken *niet* gewijzigd. Wel kan een bewijsbestand worden verplaatst of gekopieerd. De bestandkenmerken van de brondata in het verplaatste of gekopieerde bewijsbestand moeten overeenkomen met de oorspronkelijke bestandskenmerken.

2.1.2. Vastlegging van gebruikershandelingen

Veiligstellen en vorderen van gegevens gebeurt via vastgestelde procedures waarvan proces-verbaal wordt opgemaakt door de betrokken opsporingsambtenaar. In dit proces-verbaal worden onder andere de vastgestelde bestandskenmerken opgenomen.

---

[1] De *Vakbijlage Hansken* is beschikbaar op https://www.forensischinstituut.nl/vakbijlagen.

[2] Hansken haalt in meerdere stappen sporen (bijv. e-mails en foto's) uit het bewijsmateriaal. Deze verwerking van het bewijsmateriaal veranderen het bewijsmateriaal zelf *niet*.

[3] Een informatieblad '*Inzage in selecties van grote data-verzamelingen met Hansken op het NFI*' is beschikbaar op aanvraag.

[4] Zie *Vakbijlage Forensisch gebruik van bestandskenmerken en bijbehorende hashalgoritmen*, beschikbaar op https://www.forensischinstituut.nl/vakbijlagen.

3. Basisverwerking met Hansken

3.1. Een zaak aanmaken

Om de juiste gegevens aan de juiste gebruikers beschikbaar te kunnen stellen, worden bewijsbestanden per zaak gegroepeerd. Voor iedere zaak wordt één sporenverzameling aangelegd. Hiervoor maakt een functioneel beheerder in Hansken een zaak[5] aan.

3.1.1. Verwerking van het bewijsmateriaal

Bij het aanmaken van een zaak in Hansken is geen bewijsmateriaal betrokken. Hansken verwerkt in deze stap dus geen bewijsmateriaal.

3.1.2. Vastlegging van gebruikershandelingen

Voor de zaken die het NFI als dienst met Hansken ondersteunt, loopt de administratie als reguliere zaakaanvraag via het zaakadministratiesysteem van het NFI. De door de functioneel beheerders uitgevoerde handelingen vinden plaats via vaste procedures en worden per zaak vastgelegd in het zaakadministratiesysteem van Hansken.

Omdat dezelfde beheerders ook de Hansken-omgeving van de Nationale Politie functioneel beheren, volgen zij daar dezelfde procedures en leggen zij hun operationele handelingen in hetzelfde systeem vast.

Per zaak legt Hansken de volgende gegevens[6] vast:
- uniek projectnummer (binnen Hansken-omgeving[7]);
- naam van de zaak;
- aanmaakdatum en -tijd en verantwoordelijk beheerder;
- gekoppelde bewijsbestanden.

Indien ingesteld, worden de handelingen rondom het aanmaken van een zaak vastgelegd in een auditsysteem buiten de Hansken-omgeving.

3.2. Bewijsbestanden in Hansken plaatsen

De bewijsbestanden staan normaliter in de digitale onderzoeksomgeving van de opsporingsdienst. Om ze met Hansken te verwerken, moet Hansken toegang krijgen tot deze bestanden. Momenteel gebeurt dit door de bewijsbestanden te kopiëren naar een opslagruimte die specifiek voor Hansken is ingericht binnen de te gebruiken Hansken-omgeving.

De mogelijkheid bestaat om de bestanden via het interne netwerk te uploaden naar Hansken. Voor de zaken die door het NFI als dienst worden verwerkt, wordt de data via een beveiligde internetverbinding of via een fysieke transportschijf aan het NFI aangeleverd.

3.2.1. Verwerking van het bewijsmateriaal

Bij het plaatsen van een bewijsbestand in Hansken, wordt de vastgelegde brondata in het bewijsbestand (voor een snelle en veilige verwerking) gecomprimeerd en versleuteld opgeslagen in een Hansken-specifiek bewijsbestand. De brondata zelf verandert hierdoor niet. Bij ieder bewijsbestand legt Hansken vast wie het in Hansken heeft geplaatst en wanneer dat is gebeurd.

Als bestandkenmerken van de brondata in het bewijsbestand beschikbaar zijn, dan worden deze in de administratie van Hansken overgenomen.[8] Hansken biedt de mogelijkheid om na het plaatsen in Hansken, de bestandskenmerken van de gekopieerde data te controleren.

3.2.2. Vastlegging van gebruikershandelingen

Afhankelijk van de organisatie, worden verschillende procedures gevolgd voor het plaatsen van bewijsbestanden in hun Hansken-omgeving. Dit gebeurt normaliter door een digitaal expert of een functioneel beheerder van Hansken.

Voor de bewijsbestanden die het NFI als dienst met Hansken toegankelijk maakt, loopt de administratie als reguliere zaakaanvraag via het zaakadministratiesysteem van het NFI. De door de functioneel beheerders uitgevoerde handelingen vinden plaats via vaste procedures en worden per zaak vastgelegd in het zaakadministratiesysteem van Hansken.

Omdat dezelfde beheerders ook de Hansken-omgeving van de Nationale Politie functioneel beheren, volgen zij daar

---

[5] Omdat Hansken ook voor research & development wordt gebruikt, heet een *zaak* in Hansken een *project*.

[6] Voor onderzoeks- en beheerdoeleinden kunnen in Hansken aanvullende gegevens per zaak worden vastgelegd.

[7] De functioneel beheerders registreren de koppeling tussen het unieke projectnummer binnen de Hansken-omgeving en de NFI-brede zaaknummers en aanvraagnummers in het zaakadministratiesysteem van Hansken.

[8] De zogenaamde 'acquisition hashes' wordt overgenomen in de metadata van het bewijsbestand in Hansken.

dezelfde procedures en leggen zij hun operationele handelingen in hetzelfde systeem vast.

Per bewijsbestand legt Hansken de volgende gegevens vast:
- uniek ID voor het bewijsbestand (binnen de Hansken-omgeving);
- startdatum en -tijd en verantwoordelijk beheerder van het plaatsen in Hansken;
- bestandkenmerken bij veiligstellen;
- bestandkenmerken na plaatsing in Hansken.

Indien ingesteld, worden de handelingen rondom het plaatsen van bewijsbestanden vastgelegd in een auditsysteem buiten de Hansken-omgeving.

3.3. Extractie van sporen

Hansken maakt brondata in bewijsbestanden inzichtelijk door de extractie van *sporen* (bijv. bestanden, e-mails, chatberichten, foto's en documenten). Een spoor bestaat uit metadata (eigenschappen van het spoor, bijv. afzender van een e-mail of naam van een bestand), een zoekwoordenindex (woorden die voorkomen in het spoor) en de data van het spoor zelf (de bytes in de brondata). Sporen kunnen ook weer andere sporen bevatten (bijv. een *afbeelding* in een *bijlage* bij een *e-mail* in een *e-maildatabase* in een *map* in een *bewijsbestand*).[9]

In het *extractieproces* stuurt Hansken sporen herhalend naar tientallen forensische tools voor verwerking (metadata toevoegen, zoekwoordenindex vergroten en/of nieuwe sporen extraheren). Verschillende forensische tools hebben ieder hun eigen functie in dit proces (bijv. e-mails uit e-maildatabases halen, camera-informatie uit foto's halen, zoekwoorden bepalen of bestandskenmerken berekenen). Hansken plaatst de geëxtraheerde gegevens in de Hansken zoekmachine.

De data van de sporen wordt *niet* in zijn geheel opgenomen in de zoekmachine. Bij ieder spoor legt Hansken vast waar en hoe het spoor precies in welk bewijsbestand terug te vinden is.

De functioneel beheerder configureert, start en monitort dit extractieproces op basis van de aanvraag vanuit het onderzoeksteam. Hansken gebruikt hierbij een standaard set van forensische tools. Op basis van de aanvraag worden forensische tools aan- of uitgezet.

Indien gewenst, kan een extractieproces herhaald worden. Hierbij kunnen andere instellingen worden gebruik. Zo'n *herextractie* kan de eerder geëxtraheerde gegevens vervangen (bijv. bij nieuwe of andere forensische tools) of aanvullen (bijv. bij forensische tools die eerder uit stonden). Deze functie wordt ook gebruikt voor de filtering van geheimhouderstukken[10].

Als het extractieproces klaar is, controleert de beheerder of de extractie goed verlopen is en maakt de resultaten toegankelijk voor onderzoek.

3.3.1. Verwerking van het bewijsmateriaal

Een bewijsbestand wordt door Hansken beschouwd als een spoor en wordt dus ook aan forensische tools aangeboden. Als een forensische tool[11] een spoor kan verwerken, dan wordt dit in de metadata van het desbetreffende spoor vastgelegd.

Omdat tijdens een extractieproces vaak miljoenen sporen worden verwerkt, zullen er in dat proces in het algemeen ook meerdere fouten optreden. Fouten kunnen verschillende oorzaken hebben, bijvoorbeeld omdat data onvolledig is (bijv. een gedeelte van een afbeelding of PDF), omdat de structuur van de brondata niet overeenkomt met de door een forensische tool verwachte structuur (bijv. een onvolledige e-maildatabase, een nieuwe versie van een chatlog) of door omgevingsfactoren zoals overbelasting van het systeem. Hansken is echter robuust, waardoor zulke fouten worden afgevangen en bij de desbetreffende sporen worden vastgelegd.

Per spoor legt Hansken de volgende gegevens vast:
- uniek ID van het spoor (binnen de zaak en het extractieproces[12]);

---

9 Hansken beschouwt en behandelt een bewijsbestand zelf ook als spoor.

10 De functionaliteit sluit aan op de werkwijze beschreven in de 'Handleiding Verwerking geheimhouderinformatie aangetroffen in inbeslaggenomen voorwerpen en in digitale bestanden' van de Landelijke Vergadering Rechercheofficieren juni 2014. Uitgebreide uitleg is beschikbaar in het *informatieblad 'Geheimhouderinformatie Hansken'*, beschikbaar op aanvraag.

11 Het platform Hansken geeft inzicht in het gebruik van forensische tools. Dit zegt niets over de kwaliteit van deze tools en betrouwbaarheid van de door deze tools geëxtraheerde sporen. De forensische tools die met Hansken voor de Nederlandse strafrechtketen worden ingezet, zijn door het NFI ontwikkeld en/of getoetst.

12 Een herextractie van een bewijsbestand levert voor dezelfde sporen niet altijd dezelfde IDs, bijvoorbeeld omdat andere/nieuwe versies van forensische tools zijn gebruikt of de volgorde van verwerking van de sporen is gewijzigd.

- uniek ID van het bovenliggend spoor;
- forensische tool die het spoor heeft geëxtraheerd, inclusief versie-details;
- forensische tools die het spoor verwerkt hebben, inclusief versie-details en volgorde van aanroep;
- voor iedere eigenschap: forensische tool die de eigenschap heeft vastgesteld, inclusief versie-details;
- forensische tools die hebben gefaald in de verwerking van het spoor;
- relatie met de brondata in het bewijsbestand;
- berekende bestandskenmerken.

Bovenstaande gegevens maken de verwerking transparant en de sporen herleidbaar en reproduceerbaar.

3.3.2. Vastlegging van gebruikershandelingen

De functioneel beheerder configureert en start het extractieproces.

Per extractie legt Hansken de volgende gegevens vast:
- startdatum- en tijd;
- gebruikte instellingen[13]:
  - algemene instellingen voor de algehele extractie;
  - overzicht van geactiveerde forensische tools;
- instellingen per geactiveerde tool;
- algemene statistieken (bijv. aantal sporen en aantal gelezen bytes);
- statistieken per forensische tool:
  - aantal aanroepen, inclusief profiel (totale rekentijd, aantal gelezen bytes);
  - aantal gemaakte sporen;
  - aantal verwerkte sporen;
  - aantal fouten, met een samenvatting van de fouten;
  - ongebruikte forensische tools (tools die wel geactiveerd zijn, maar geen sporen hebben verwerkt).

Bovenstaande gegevens maken het mogelijk de extractie nogmaals uit te voeren. De statistieken ondersteunen de controle van een (her)extractie en geven richting aan de (door)ontwikkeling van Hansken en de forensische tools.

Indien ingesteld, worden de handelingen rondom het extraheren van sporen vastgelegd in een auditsysteem buiten de Hansken-omgeving.

4. Gebruik voor zaakonderzoek

4.1. Doorzoeken van de sporenverzameling

De in de zoekmachine van Hansken vastgelegde sporen kunnen handmatig (via de gebruikersinterfaces) of geautomatiseerd (met een script) doorzocht worden.

Zoeken kan op verschillende manieren:
- door het filteren op de metadata (bijv. alleen afbeeldingen, e-mails van een bepaalde afzender of documenten geprint in een bepaalde periode);
- door het gebruiken van de zoekwoordenindex (bijv. sporen waar een bepaald woord in voor komt).

Deze zoekfuncties kunnen worden gecombineerd, zodat bijvoorbeeld gezocht kan worden naar e-mails waar bepaalde woorden in voorkomen en die zijn verstuurd in een bepaalde periode.

Bij ieder spoor is vastgelegd waar het spoor precies in welk bewijsbestand terug te vinden is. Als een gebruiker van Hansken een spoor wil inzien, dan wordt dit spoor (bijv. de e-mail, het Office-document of de afbeelding) op dat moment uit het bewijsbestand gekopieerd.

Het combineren van digitale sporen in Hansken met gegevens buiten Hansken vindt plaats buiten de Hansken-omgeving.

4.1.1. Verwerking van het bewijsmateriaal

In deze onderzoekstap wordt slechts gezocht in de al beschikbare sporenverzameling. De sporen in deze verzameling kunnen niet worden aangepast.

Gebruikers kunnen wel notities en labels aan sporen toevoegen die gebruikt worden voor onderzoek-specifieke doeleinden (bijv. voor het vastleggen van relevante sporen of het markeren van sporen waar vervolgonderzoek op moet plaatsvinden).

4.1.2. Vastlegging van gebruikershandelingen

Bij notities wordt vastgelegd wie wanneer de notitie bij een spoor heeft geplaatst. Dit geldt niet voor labels.

Indien ingesteld, worden de handelingen rondom het doorzoeken van sporenverzamelingen vastgelegd in een auditsysteem buiten de Hansken-omgeving.

[13] Instellingen worden vastgelegd wanneer deze afwijken van de standaardinstellingen.

4.2. Vervolgverwerking van sporen

Het komt regelmatig voor dat er vervolgverwerking plaatsvindt van sporen die door Hansken inzichtelijk zijn gemaakt, bijvoorbeeld wanneer nieuwe formaten worden aangetroffen waar Hansken (nog) geen ondersteuning voor heeft (bijv. een database met chatberichten van een nieuwe chat-app).

Hansken biedt de mogelijkheid om sporen van buitenaf in Hansken te plaatsen. Dit vindt typisch plaats door digitaal experts. Sporen die op deze manier in Hansken worden geplaatst, worden opgenomen in de zoekmachine van Hansken. Deze zijn dan ook doorzoekbaar, net als de met Hansken door de forensische tools vastgestelde sporen. De verantwoordelijkheid voor deze sporen ligt bij de gebruiker die ze in Hansken heeft geplaatst. Daarom kunnen deze sporen ook worden aangepast en overschreven.

4.2.1. Verwerking van het bewijsmateriaal

De vervolgverwerking van het bewijsmateriaal (en de vastlegging daarvan) vinden plaats buiten Hansken.

4.2.2. Vastlegging van gebruikershandelingen

De sporen die op deze manier in Hansken worden geplaatst en/of aangepast, worden gemarkeerd. In de rapportage van zo'n spoor wordt opgenomen dat dit spoor door een gebruiker is toegevoegd.

Per spoor dat op deze manier in Hansken is geplaatst, legt Hansken de volgende gegevens vast:

- gebruiker die het spoor in Hansken heeft geplaatst en/of aangepast;
- datum en tijd waarop het spoor in Hansken is geplaatst en/of aangepast;
- omschrijving van de verwerking van het spoor;
- de toegevoegde, aangepaste en/of verwijderde eigenschappen;
- de oude en nieuwe waarde van eigenschappen (bij aanpassingen).

Indien ingesteld, worden de handelingen rondom het plaatsen en/of later aanpassen van sporen vastgelegd in een auditsysteem buiten de Hansken-omgeving.

Voor algemene vragen kunt u contact opnemen met de Frontdesk, telefoon (070) 888 68 88. Voor inhoudelijke vragen kunt u contact opnemen met het onderzoeksgebied Forensische Digitale Technologie, specialisatie data-analyse van de afdeling Digitale en Biometrische Sporen.

telefoon (070) 888 6400.

Nederlands Forensisch Instituut

Ministerie van Justitie en Veiligheid

Postbus 24044 | 2490 AA Den Haag

Telefoon (070) 888 66 66

www.forensischinstituut.nl

november 2021.