Nederlands Forensisch Instituut
Ministerie van Justitie en Veiligheid

Inzage in selecties van grote data-verzamelingen met Hansken op het NFI

3 maart 2021

informatieblad

Nederlands Forensisch Instituut

Postadres
Postbus 24044
2490 AA Den Haag

Bezoekadres
Laan van Ypenburg 6
2497 GB Den Haag
T (070) 888 66 66
F (070) 888 65 55

www.forensischinstituut.nl

Inhoudsopgave

1	Aanleiding	3
2	Inleiding	3
3	Basisverwerking met Hansken	4
	3.1 Brondata	4
	3.2 Extractie van sporen	4
	3.3 Filteren van geheimhoudersstukken	4
	3.4 Doorzoeken van de sporenverzameling	5
4	Filteren van deelverzamelingen	5
5	Inzage via Hansken op het NFI	6

75003

1 Aanleiding

In meerdere zaken krijgen advocaten inzage in digitaal bewijsmateriaal. In gevallen waarbij slechts een selectie van grote dataverzamelingen ter inzage worden aangeboden, kan inzage plaatsvinden op het NFI met Hansken.

Dit informatieblad geeft antwoord op de vraag waarom deze inzage op het NFI moet plaatsvinden en niet mogelijk is vanaf bijvoorbeeld het kantoor van de advocaat.

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) 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 (zonder IT-specialisatie) die geautoriseerd zijn voor onderzoek aan deze stukken van overtuiging. 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.

Je kan met de forensische dienst de zoekresultaten blijven filteren totdat je van die miljoenen sporen een beheersbare selectie overhoudt, waarvan de sporen één voor één te bekijken zijn.

Sinds 2018 wordt Hansken regelmatig ingezet om naast de onderzoeksteams ook andere strafprocespartijen toegang tot de data geven, waaronder advocaten van verdachten. In dit informatieblad wordt toegelicht waarom en hoe deze inzage op het NFI wordt georganiseerd.

Voor de verwerking van data met Hansken wordt onderscheid gemaakt in twee soorten data-verzamelingen:

- Data die voor één specifieke zaak beschikbaar is en onderzocht mogen worden, bijvoorbeeld data uit de inbeslaggenomen smartphone en computer van de verdachte;
- Data die voor meerdere zaken van belang kan zijn en waarvan een deel voor een zaak onderzocht mag worden, bijvoorbeeld gevorderde data uit servers voor de communicatie tussen cryptophones.

Voor beide varianten vindt een basisverwerking plaats met Hansken, zie hoofdstuk 3. Als slechts een deel van een data beschikbaar mag zijn voor een zaakonderzoek (en dus ook voor inzage), dan worden aanvullend op de basisverwerking filters toegepast, zie hoofdstuk 4.

Inzage in zulke deelverzamelingen vindt plaats op het NFI, zie hoofdstuk 5 voor een toelichting.

75003

3 Basisverwerking met Hansken

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

3.1 Brondata

De brondata is de data-verzameling die uit de inbeslaggenomen apparaten is veiliggesteld of is gevorderd bij bijvoorbeeld providers. Het veiligstellen van deze brondata vindt plaats in zogenaamde bewijsbestanden, ook wel images genoemd. Dit gebeurt via vastgestelde procedures waarvan proces-verbaal wordt opgemaakt. Om de integriteit van deze data te borgen, worden bij het veiligstellen bestandskenmerken[2] berekend, ook wel hashes of hashtotals genoemd. Deze bestandkenmerken zijn reproduceerbaar en worden opnieuw berekend als een bewijsbestand bijvoorbeeld wordt verplaatst of gekopieerd. De bestandkenmerken van het verplaatste of gekopieerde bewijsbestand moeten overeenkomen met de oorspronkelijke bestandskenmerken.

3.2 Extractie van sporen

Om een bewijsbestand met Hansken te doorzoeken, wordt momenteel een kopie in Hansken geplaatst (met integriteitscontrole op basis van de bestandskenmerken).

Tijdens het extractieproces wordt met Hansken deze brondata inzichtelijk gemaakt. Dit houdt in dat de data wordt aangeboden aan forensische tools die (herhalend, op basis van de structuur van de data) digitale sporen in de data herkennen, indexeren en opnemen in de Hansken zoekmachine. Daarna kan de sporenverzameling doorzocht worden.

3.3 Filteren van geheimhoudersstukken

Bij het veiligstellen van de brondata (maken van een image) is het lastig of onmogelijk om geheimhoudersstukken uit te sluiten, bijvoorbeeld enkele e-mails in een grote database. Dit doorkruist het forensische proces en het daadwerkelijke onderzoek aan de brondata vindt in een later stadium plaats.

Als verwacht wordt dat geheimhoudersstukken in de brondata voorkomen, dan kan daar tijdens het extractieproces met Hansken wel rekening mee worden gehouden. Als specifieke zoektermen in digitale sporen voorkomen (bv. de naam of contactgegevens van de advocaat), dan kunnen deze sporen gemarkeerd en ontoegankelijk gemaakt worden (op basis van black-listing). Dit is gelijkgesteld met vernietiging in het *Besluit bewaren en vernietigen niet gevoegde stukken*.

White-listing en black-listing

Bij het filteren van een sporenverzameling wordt de verzameling in tweeën gesplitst, vergelijkbaar met een zeef: sporen die voldoen aan het filter blijven in de zeef achter, sporen die niet voldoen vallen erdoorheen.

Bij white-listing blijven alleen de sporen over die voldoen aan het filter (en dus die in de zeef achterblijven).

Bij black-listing worden de sporen die voldoen aan het filter (en dus in de zeef achterblijven) weggegooid en blijft de rest dus over.

In beide gevallen bestaat de kans op vals-positieven en vals-negatieven.

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

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

75003

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*.

Om technische redenen kan zo'n gemarkeerd spoor meestal *niet* uit de brondata verwijderd worden, bijvoorbeeld omdat het spoor is gevonden na meerdere analysestappen (bv. een afbeelding in een bestandsarchief in de bijlage van een e-mail) of omdat het spoor onderdeel uitmaakt van een groter geheel (bv. een chatbericht in een chatlog).

Als de brondata wordt aangepast (door sporen te verwijderen), kan ook de integriteit van deze brondata niet altijd meer gecontroleerd worden.

3.4 Doorzoeken van de sporenverzameling

De meta-data van de sporen worden in de zoekmachine opgenomen (bv. de afzender van een e-mail, de naam van een digitale afbeelding of de auteur van een Office-document). Daarnaast worden alle woorden die in een spoor voorkomen opgenomen (bv. in een e-mail, chatbericht of Office-document).

De sporen zelf worden *niet* in zijn geheel opgenomen in de zoekmachine. Bij ieder spoor wordt vastgelegd waar het spoor precies in welk bewijsbestand terug te vinden is. Als een onderzoeker (of advocaat) het spoor wil inzien, dan wordt dit spoor (de e-mail, het Office-document of de afbeelding) op dat moment uit het bewijsbestand gehaald.

4 Filteren van deelverzamelingen

Als slechts een deel van een data beschikbaar is voor een zaakonderzoek (en dus ook voor inzage), dan worden aanvullend op de basisverwerking filters toegepast.

Voor nieuwe deelverzamelingen (subsets), worden géén nieuwe extracties uitgevoerd. De sporen (metadata en woorden) in zo'n deelverzameling worden uit de vooraf geëxtraheerde sporenverzameling (de basisset) gekopieerd.

Selectie van de sporen in een deelverzameling vindt plaats op basis van white-listing filters, waarbij het filter wordt ingesteld op basis van zoektermen.

Over het algemeen zal, afhankelijk van de toegepaste bevoegdheden, een rechter-commissaris of officier van justitie besluiten over de toe te passen filters.

75003

5 Inzage via Hansken op het NFI

Het verzorgen van inzage door een deel van het materiaal beschikbaar te stellen op een gegevensdrager of gegevensbestand is mogelijk en gebeurt ook in de praktijk. Hierbij ontbreken echt de zoekmogelijkheden van Hansken en kan *niet* direct in de brondata gezocht worden. Dit is voor de beoordeling en forensische duiding van sporen wel van belang. Deze beschikbaarstelling moet dan ook worden beschouwd als een extra hulpmiddel en tegemoetkoming aan de behoeften van de verdediging.

Hansken is een handig hulpmiddel om grote deelverzamelingen in beperkte tijd te doorzoeken *met* directe toegang tot de brondata. Dit geldt ook voor de verdediging. Inzage kan dan ook via Hansken plaatsvinden. Er zijn drie redenen om deze inzage via Hansken vooralsnog op het NFI te organiseren:

1. **De brondata kan niet volledig uitgeleverd worden**
   Zoals eerder uitgelegd, worden bij een deelverzameling een selectie van de sporen opgenomen in de zoekmachine van Hansken. Om de inhoud van deze sporen te kunnen bekijken, is de brondata nodig. Deze brondata bevat ook de data van de uitgefilterde sporen, die dus niet voor het onderzoek beschikbaar is. Daarom kan de brondata niet volledig uitgeleverd worden.

   Er bestaat momenteel geen technische mogelijkheid om de inhoud van enkel de sporen in zo'n deelverzameling uit de brondata te halen en aan te bieden voor inzage op locatie met Hansken.

2. **Hansken is niet toegankelijk vanaf een willekeurige locatie**
   Hansken is een platform dat deelverzamelingen doorzoekbaar kan maken, waarbij Hansken de data centraal opslaat. Om veiligheidsredenen is het momenteel niet mogelijk Hansken vanaf een willekeurig apparaat op een willekeurige locatie op afstand te gebruiken.

   Er loopt een project om deze inzage door advocaten met Hansken via een beveiligde verbinding te laten lopen, zodat dit wel op afstand kan plaatsvinden.

3. **Inzage bij de opsporingsdiensten is ongewenst**
   Vanuit de advocatuur is aangegeven dat inzage in de data bij voorkeur niet plaatsvindt in de systemen bij de opsporingsdiensten omdat hiermee mogelijk ongewenst informatie beschikbaar komt voor de opsporingsdiensten.

75003