Kennis- en Onderzoeksagenda Digitaal

Doel

De kennis- en onderzoeksagenda Digitaal Forensisch Onderzoek richt zich de ontwikkeling van nieuwe methoden, tools en procedures voor het verkrijgen en verwerken van digitaal materiaal ten behoeve van de opsporing en bewijsvoering in strafzaken.

Focus

Het digitaal forensisch werkveld is gigantisch breed en verandert dagelijks met de komst van nieuwe en verbeterde apparaten en nieuwe apps en softwaretoepassingen.
Om keuzes te kunnen maken en focus aan te brengen werken we enerzijds vanuit de wetenschap en technologie en anderzijds vanuit het zaakmateriaal. We richten ons op herbruikbaarheid en zaaksimpact van de R&D resultaten:

Lage diversiteit
veelvoorkomende onderdelen, interfaces en protocollen en veelgebruikte datastructuren;

Veel voorkomendheid in onderzoeksmateriaal
onderdelen/data in specifieke systemen en in zaken;

Grote zaakimpact
veel tactische informatie en/of een hoge bewijswaarde.

Scope

Data verkrijgen

Een grote uitdaging is het toegang verkrijgen tot data in gesloten omgevingen. Deze omgevingen bestaan uit fysieke (consumenten)apparaten, van smartphone tot serverpark, en online diensten, bijvoorbeeld Dropbox of Gmail. Toegang wordt op verschillende manieren beperkt, in de praktijk zien we dat hier vooral versleuteling (cryptografie) voor wordt ingezet. De algoritmen zijn sterk en steeds vaker worden sleutels in losse, goed beveiligde (hardware)componenten vastgelegd.

Data verkrijgen uit apparaten
We proberen beveiligingen te omzeilen door gebruikte hardware en software te analyseren en te beïnvloeden.
We richten ons op het verkrijgen van toegang tot hardwarecomponenten waar onbeveiligde data afgetapt kan worden of waar informatie beschikbaar is die helpt bij het verkrijgen van toegang tot opgeslagen data.
We werken continu aan de doorontwikkeling van de Memory Toolkit II, een apparatuur om geheugenchips te analyseren en de data uit te lezen.

Data verkrijgen uit online omgevingen
We ontwikkelen methoden en tools om op een forensisch betrouwbare manier gegevens uit online diensten veilig te stellen.

Ontsleuteling van data
We onderhouden een rekencluster voor de ondersteuning bij het ontsleutelen van versleutelde data, ook wel ontcijfering of decryptie genoemd.
We werken aan methoden en tools om wachtwoorden en sleutels te achterhalen in de data, die helpen bij het veiligstellen en inzichtelijk maken van versleutelde data.

Data betekenis geven

Zodra niet-versleutelde data beschikbaar is, moet deze inzichtelijk gemaakt worden. Om de betekenis van de data te achterhalen, analyseren we de structuur van de data. Op basis van bekende

datastructuren vertalen we data naar digitale objecten (ofwel sporen) zoals e-mails, afbeeldingen en documenten. Door de snelle ontwikkeling van digitale apparaten en apps, wordt data continu op nieuwe manieren gestructureerd.

Data structureren

Om data geautomatiseerd inzichtelijk te maken worden voortdurend nieuwe datastructuren beschreven in herbruikbare forensische softwarebibliotheken.
We werken aan een domein-specifieke taal voor het vastleggen van deze structuren zodat ze snel, overzichtelijk en goed onderhouden kunnen worden.

Herkennen met kunstmatige intelligentie

Naast het vaststellen van sporen op basis van datastructuren, analyseren we digitale objecten op basis van kunstmatige intelligentie, bijvoorbeeld om entiteiten in teksten of objecten in afbeeldingen te herkennen. Ook deze technieken worden vastgelegd in herbruikbare forensische softwarebibliotheken.
We onderzoeken de betrouwbaarheid en reproduceerbaarheid van technieken voor intelligente dataverwerking ten behoeve van de opsporing en bewijsvoering.

Sporen inzichtelijk maken

In hedendaagse strafzaken zie we de hoeveelheid digitaal materiaal toenemen, waarbij niet alles meer gezien en onderzocht kan worden. Een slimme selectie is nodig.

Gestructureerde data beschikbaar stellen

Alle kennis die we vastleggen is er primair op gericht om grootschalig ingezet te worden. Hiervoor ontwikkelen we het digitaal forensisch onderzoeksplatform Hansken.
Met Hansken kunnen ketenpartners zelf inbeslaggenomen of gevorderde data verwerken door toepassing van de in de forensische softwarebibliotheken vastgelegde kennis op basis van datastructuren en kunstmatige intelligentie.

Sporen aggregeren en visualiseren

We werken aan verbeterde presentatie, filtering en aggregatie van grote verzamelingen digitale sporen, onder meer door ons te richten op het vastleggen en inzichtelijk maken van relaties tussen sporen. Relaties worden vastgesteld op basis van referentie-experimenten en/of met behulp van neurale netwerken.

Sporen duiden en evalueren

Om digitale sporen als bewijsmiddel in te brengen, is het cruciaal dat de betekenis van de sporen binnen de zaak duidelijk zijn. Met andere woorden, de sporen moeten geduid worden. Daarnaast is het belangrijk om de sporen te koppelen aan activiteiten van individuen, bijvoorbeeld een verdachte.

Duiding van sporen

We leggen vast hoe je digitale sporen kunt combineren om tot nieuwe inzichten te komen. Om de betekenis van sporen te achterhalen, richten we ons op het automatiseren van experimenten. Deze experimenten leren ons welke sporen worden achtergelaten als specifieke handelingen met digitale apparatuur worden uitgevoerd.
Om uitspraken te kunnen doen over uitgevoerde handelingen op een digitaal apparaat, werken we aan theoretische onderbouwing voor deze bewijswaardering op basis van formele methoden en kunstmatige intelligentie.
We werken aan methoden en tools om deze betekenis inzichtelijk te presenteren aan zaakonderzoekers.
We onderzoeken of door goede toepassing van anonimisatie en de-identificatie deze referentiegegevens ook door ketenpartners of anderen verzameld kunnen worden.

Kwaliteit en procedures

Methoden en tools worden gebruikt ten behoeve van de opsporing en bewijsvoering. Hierbij moeten alle sporen herleidbaar zijn naar een inbeslaggenomen of gevorderde bron (chain of evidence) en het moet duidelijk zijn welke handelingen zijn uitgevoerd (chain of custody).

Standaard voor beschrijven en uitwisselen van sporen

In een breed internationaal consortium ontwikkelen we een standaard (CASE) voor het beschrijven van digitale sporen inclusief hun bewijsketens (chains of evidence and custody), zodat ze ten behoeve van bewijsvoering tussen jurisdicties uitgewisseld kunnen worden.

Referentiedata voor validatie van tools

In een breed internationaal consortium (ValiD) werken we aan een dataverzameling ten behoeve van de validatie van digitaal-forensische tools.

Kader

Het kader legt vast aan welke voorwaarden projecten moeten voldoen die een bijdrage leveren aan de implementatie van deze kennis- en onderzoeksagenda. De criteria vallen onder het 'pas toe of leg uit' (ptolu) principe.

Verbinding

- Minstens 1 externe organisatie is betrokken.
- De (vergaring van de) eisen en wensen van de eindgebruiker van de projectresultaten maken onderdeel uit van het projectplan en worden in het project getoetst (vraaggestuurd werken).
- De impact op de strafrechtketen bij het succesvol afronden van het project is beschreven.

Kennisdeling en communicatie

- Kennis die wordt opgedaan in het project wordt vastgelegd en beschikbaar gesteld via een (ketenbreed) platform.
- Zowel de documentatie van methoden en procedures als de automatisering in bibliotheken, tools en gebruikers-interfaces wordt gedeeld.

Organisatie

- Het project maakt gebruik van beschikbare specialisaties binnen de divisie, waaronder infrastructuur- en systeembeheer en softwareontwikkeling.
- Gemaakte afspraken binnen specialisaties gelden voor het project.

Forensische toepassing

- Borging en validatie van de eindresultaten maken expliciet onderdeel uit van het project.

Juridische context

- De juridische context, waaronder (privacy)beperkingen en bevoegdheden, maken onderdeel uit van het projectplan.
- Benodigde bevoegdheden zijn bij aanvang van het project geregeld.

Duurzaamheid

- Het project richt zich op de inzet van bestaande technologie of de ontwikkeling van herbruikbare technologie.
- Projectresultaten zijn inzetbaar voor meerdere zaken of leveren een bijdrage aan andere innovatieprojecten.