Auteur: Jos Griffioen is docent/onderzoeker bij het lectoraat Digital Forensics & E-Discovery. Hij is o.a. docent bij de Master Digital Forensics en de bachelor Forensisch ICT. Jos is meer dan 40 jaar werkzaam in de ICT waarvan 23 jaar in het digitaal forensisch onderzoeksdomein. Hij is bereikbaar via: griffioen.j@hsleiden.nl.

Wouter Keuris Fotografie

Forensisch ICT: een andere manier van kijken naar informatica

Hogeschool Leiden leidt al vijftien jaar studenten op tot forensisch ICT'er. Was er in eerste instantie enkel een voltijds bachelor uitstroomrichting, in 2020 kwam er een deeltijd variant bij. In 2023 is de deeltijd masteropleiding gestart en vanaf september 2025 start ook de voltijds master. De belangstelling groeit voor deze aparte richting van ICT. Het nut en de noodzaak groeit ook. Wat maakt dit vakgebied en vooral ook het onderwijs daarin zo bijzonder?

Wat verstaan we onder digitaal forensisch onderzoek? 'In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony.' (1)

Vandaag de dag zijn er bij elk delict wel digitale sporen aanwezig (2) die steeds vaker binnen de rechtsgang als bewijs worden gebruikt. Het belang van meer en goed opgeleide digitaal forensisch onderzoekers neemt hiermee toe.

Het herkennen, vastleggen en analyseren van deze sporen is een vak apart. Alhoewel digitaal rechercheren vanzelfsprekend in de basis alles van doen heeft met ICT, zijn de benodigde skills veel breder: digitale data dient behandeld te worden als DNA, verandering van opslag of inhoud kan desastreus zijn voor de bewijswaarde. De sporen gaan vooral over activiteiten en gedrag, gerepresenteerd in bits en bytes. Het onderkennen van dit gedrag is essentieel. Technische onderzoeksmogelijkheden zijn soms juridisch niet toegestaan: het is vaak onderzoeken met één arm op de rug.

In 2009 besloot Hogeschool Leiden een specialisatie Forensisch ICT op te zetten binnen de opleiding Informatica. Na een gezamenlijke propedeuse kunnen studenten, naast Software Engineering, Business IT en Mediatechnologie ook kiezen worden voor Forensisch ICT. In september 2010 zaten de eerste zestien studenten hoopvol in de klas: nu ging het gebeuren, CSI werd werkelijkheid! De waarheid was weerbarstiger. Het bleek dat bijvoorbeeld hardware- en netwerktechnologie toch wel erg belangrijk zijn, om überhaupt met het speuren te kunnen beginnen. Daarnaast was programmeren (met name Python) toch het Zwitsers zakmes van de gemiddelde digitaal rechercheur. Alhoewel een lokaal dagblad iets kopte als 'Hogeschool gaat hackers opleiden', leek de werkelijkheid toch meer op een reguliere Informatica-opleiding, waarbij wel alle aspecten van de informatica even belangrijk bleken, echter vaak op een net andere manier bekeken! Door de jaren heen groeide het aantal belangstellenden gestaag. In de huidige bacheloropleidingsvariant, direct startend in de propedeuse, zien we nu meer dan zestig aanmeldingen.

Onderzoek en multidiscipline

Kenmerkend voor de opleiding tot forensisch ICT'er zijn de voortdurende nadruk op het doen van goed onderzoek (waarheidsvinding) en het respecteren van de juridische en ethische kaders. In het proces van data naar bewijs dient een voortdurende verificatie plaats te vinden of de gevonden data daadwerkelijk te vertalen is naar de gevraagde informatie en kan dienen als juridisch bewijs. Alhoewel er veel goede analysetools beschikbaar zijn, blijken deze door de constante veranderende technologie regelmatig toch niet te voldoen. Denk bijvoorbeeld aan de snelle updates van apps en OS-en, waardoor analysesoftware geen of verkeerde informatie ophaalt uit de te onderzoeken data. De digitaal rechercheur zal dan zelf de nieuwe structuren onderzoeken om vervolgens met behulp van eigen software alsnog de waarheid boven tafel te krijgen.

Deze zeer specialistische kennis dient op een zodanige wijze te worden overgedragen, dat een meestal niet technisch onderlegde doelgroep hiermee verder kan: de juristen. Een innige samenwerking tussen deze twee verschillende beroepsgroepen is noodzakelijk om enerzijds op juridisch correcte wijze bewijs te kunnen abstraheren en anderzijds dit bewijs zodanig te presenteren, dat ook niet-ingewijden in de 'diepere ICT' hier vervolgens conclusies uit kunnen trekken! Daarnaast gaat ethiek ook een steeds belangrijkere rol spelen, denk bijvoorbeeld aan de inzet van AI binnen opsporing (gezichtsherkenning), privacy, maar ook de ethische kanten van het behandelen van onderzoeksdata (big data) en resultaten.

Voortdurende aanpassing

De digitalisering van onze samenleving en de voortdurende vernieuwing van de technologie hebben een sterke invloed op het digitaal forensisch onderwijs (3). In 2007 verscheen de eerste iPhone en in 2008 de Android Phone. Dit was een revolutie in onze samenleving, maar ook voor digitaal forensisch onderzoek. In plaats van onderzoek op thuiscomputers of servers kwam er heel veel informatie beschikbaar via die kleine zwarte doosjes: e-mail, contacten, foto's, browsergeschiedenis, locaties etc. Begonnen we in 2010 in Leiden redelijk traditioneel met vakken als Computer Forensics, Network Forensics en E-Discovery, door de jaren heen moest het curriculum voortdurend worden bijgesteld.

Door de opkomst van IoT en andere embedded toepassingen (bijvoorbeeld in de automotive) wordt de kennis van de technische informatica en elektronica crucialer voor de digitaal rechercheur. Zonder diepgaande kennis van analoge naar digitale technieken, kan de gevonden informatie niet op zijn juiste waarde worden ingeschat. Iedereen kent wel het voorbeeld van een totaal foutieve gps-locatie in een foto door externe beïnvloeding van het gps-ontvangstsysteem. Tegelijkertijd wordt door exponentiële groei van dataskills, datascience een belangrijk wapen. De huidige opmars van AI in de samenleving zien we vanzelfsprekend ook terug in het digitaal forensisch domein. Die biedt kansen door gebruik van AI in opsporing, maar geeft ook nieuwe uitdagingen. Bij gebruik in de opsporing kan de transparantie van bewijsvergaring onder

druk komen te staan. Daarnaast is het herkennen van gebruikte AI, bijvoorbeeld bij deepfakes of specifieke anti forensics technieken niet eenvoudig. Dit kat-en-muis spel is normaal in de wereld van opsporing: nieuwe technologie zorgt voor nieuwe criminaliteit, maar ook voor nieuwe opsporingskansen.

In dit alles veranderen onze opleidingen continu mee, waarbij drie zaken wel gelijk blijven: onderzoek en juridische affiniteit blijven de hoofdrol spelen. Als derde het bovengenoemde kat-en-muisspel; onze studenten worden voortdurend getraind in het zoeken naar nieuwe mogelijkheden.

Mede door het onderzoek vanuit het in 2016 opgerichte lectoraat Digital Forensics & E-Discovery (4) en een nauwe band met de academische Digital Forensics wereld (DFRWS) (5) zijn we in staat deze veranderingen steeds tijdig te blijven inzetten. Studenten van onze master gaan hier vanzelfsprekend ook een belangrijke rol in spelen. Bachelorstudenten studeren nu al af in lectoraat onderzoeksprojecten of werken tijdens stage mee en geven vorm aan eigen onderzoeksprojecten.

Werkveld

Vanaf het begin is het werkveld sterk betrokken bij de opleidingen. Niet alleen de Nationale Politie, NFI of FIOD, maar zeker ook de grote accountancykantoren, cybersecuritybedrijven (DFIR) en recherchebureaus. Samenwerking op het gebied van projectonderwijs, hackatons, gastcolleges of het leveren van hybride docenten.
De opleiding heeft een strategische samenwerking met het NFI, waardoor we gezamenlijk de nieuwste thema's kunnen duiden en een bijdrage leveren aan onderzoek. Voorbeelden hiervan zijn Hansken (6) en Aardwolf (7). Hansken is het digitale zoekplatform van het NFI en wordt gebruikt in ons onderwijs. Door middel van hackatons kunnen studenten extra functionaliteit bouwen. Daarnaast wordt medewerking verleend aan het EU-project Aardwolf, een appsanalyse en referentiedatabase, die de voortdurende updates van meest gebruikte apps bijhoudt. Hierdoor weet een rechercheur veel sneller op welke wijze en waar bepaalde benodigde data is opgeslagen. Zowel bachelor- als masterstudenten werken hieraan mee.

Doelgroep opleidingen

Vanzelfsprekend is de voltijd bachelor forensisch ICT gericht op de middelbare scholier, die een carrière in het private of publieke domein als digitaal forensisch onderzoeker ambieert. Sommigen worden liever ontwikkelaar van forensische software en enkelen gebruiken hun talenten in het onderwijs en geven les op onze eigen hogeschool.
De deeltijd bachelor is opgezet voor mensen die al werkzaam zijn in het werkveld. Met behulp van deze studie kunnen ze hun specifieke skills uitbreiden naar het niveau van een volledige bachelor. De combinatie van ervaring, werk en onderwijs kan de reguliere studieduur van een bachelor doen verkorten. We zien tot nu toe vooral een instroom vanuit opsporingsdiensten. Er zijn zeker goede aansluitingsmogelijkheden voor werknemers vanuit bijvoorbeeld de cybersecurity (DFIR).
Ook de deeltijd master is gericht op deelnemers werkend in het digitaal forensisch domein. Zij willen zich bezighouden met innovatie: (wetenschappelijk) onderzoek en strategie. Of ze willen beter opgeleid zijn om zeer complexe digitaal forensisch onderzoeken uit te voeren of aan te sturen. Vooraf is een maatwerk pre-master beschikbaar om tot het juiste instapniveau te komen.
De voltijd master is als eerste een kopstudie boven op onze eigen bachelor, maar kan zeker ook worden gevolgd door andere hbo-ICT studenten (bijvoorbeeld cybersecurity). Deze studenten zullen eerst een pre-master moeten volgen.

Toekomst

Vandaag is het AI wat de hoofdrol speelt, morgen is het misschien wel quantum-computing, hybride intelligentie of cybernetica. Allen met eigen uitdagingen: technisch, juridisch en ethisch. Door de nauwe band tussen ons lectoraat en de diverse opleidingen kunnen tijdig nieuwe trends worden opgemerkt en worden verwerkt in onderwijs. De voortdurend veranderende technologie vereist continu bijgeschoolde digitaal forensisch onderzoekers. Deeltijdopleidingen kunnen een rol spelen in deze bijscholing. Daarnaast zijn diverse mastermodulen nu ook los te volgen als microcredentials (8). De vraag naar specifiek werkveldgericht onderwijs zal enkel toenemen, niet alleen in het digitaal forensisch domein. Een hele uitdaging voor onderwijzend Nederland. Samenwerking zou hierbij kunnen helpen. De toenemende noodzaak van kennis van Digital Forensics binnen cybersecurity heeft ervoor gezorgd, dat Hogeschool Leiden een module Digital Forensics binnen de

Master Cybersecurity Engineering van de Haagse Hogeschool gaat vormgeven. Tegelijkertijd gaat de Haagse Hogeschool een module Malware & Hacking voor onze Master Digital Forensics verzorgen. Op deze wijze maken we optimaal gebruik van de schaarse experts en kan men de bespaarde tijd gebruiken voor nieuw onderzoek en hernieuwing van bestaand onderwijs.

Forensisch ICT is een vakgebied dat een sterke band heeft met disciplines als onderzoek, wetgeving en ethiek. Technologische ontwikkelingen volgen is een voortdurende uitdaging. Als Hogeschool Leiden lukt ons dat door eigen onderzoek via een lectoraat in zowel bachelor- als masteronderwijs en door een goede samenwerking met toonaangevende partijen uit de publieke en private sector.

Referenties

(1) NIST https://csrc.nist.gov/glossary/term/digital_forensics

(2) R. Zuurveen, W. Ph. Stol Benutten van Digitale sporen (2020) https://www.politieenwetenschap.nl/publicatie/politiekunde/2020/benutten-van-digitale-sporen-359

(3) Henseler, H. De (R)evolutie van Digitaal Bewijs. Lectorale rede. 21 november 2017

(4) Lectoraat DF&ED https://www.hsleiden.nl/digital-forensics

(5) Digital Forensics Research Workgroups https://dfrws.org

(6) https://www.hansken.nl

(7) https://aardwolfproject.eu

(8) https://education.ec.europa.eu/nl/education-levels/higher-education/micro-credentials