Hans Heins, Specialist Digitaal Rechercheren: "Digitaal rechercheren is geen hobby, maar een vak!"

Hans Heins is 45 jaar en 2,5 jaar werkzaam als Specialist Digitaal Rechercheren bij de Vakgroep Informatie Recherche op het LSOP (Landelijk Selectiecentrum Opleiding Politie) in Zutphen; beter bekend als de Rechercheschool.
Naast zijn werk is hij een fervent motorrijden en trotse bezitter van een Pan European, ook is hij actief in een zwemclub als trainer van wedstrijdzwemmers. In 1999 is hij begonnen bij het LSOP……..

Loopbaan
Na het behalen van zijn CIOS diploma heeft hij, om sportinstructeur te kunnen worden bij de politie, de Politie Opleiding gevolgd in Amersfoort. In 1979 werd hij, na het voltooien van zijn opleiding, geplaatst in Hazerswoude. Na 2,5 jaar gewacht te hebben op een plek als sportinstructeur, kwam hij bij de recherche terecht. Zijn wens om sportinstructeur viel in duigen toen hij geplaagd werd door een hernia, maar hij bleef geboeid door het recherchewerk. Voordat Hans, door een reorganisatie, terecht kwam bij de districtsrecherche Hollands Midden, was hij ongeveer 12 jaar werkzaam met fulltime tactisch recherchewerk als groepsrechercheur. In 1994 werd hij uitgeleend aan het team computercriminaliteit Haaglanden, een van de drie korpsen computercriminaliteit, waar hij in totaal 5 jaar gewerkt heeft.
In 1999 is hij begonnen bij het LSOP als Specialist Digitaal Rechercheren, waar hij naast het digitaal rechercheren ook twee lesblokken van de vervolgcursus Digitaal Rechercheren en Internet (tools en sporen) geeft. Soms geeft hij ook les in bewustwording.

Geschiedenis Digitaal Rechercheren
Tijdens zijn werk bij het team computercriminaliteit, waarbij hij zich 4 jaar lang bezig gehouden heeft met onderzoek en huiszoekingen, gebruikten zij een soort koelkastmodel laptop. Software als EnCase was er toen nog niet , dus gebruikten zij voor computeronderzoek de volgende software: diskedit, disksearch en novabreak. Ze probeerden altijd terplekke een backup te nemen, maar door de verschillende systemen ging dit niet altijd. Het onderzoeken van pc's leverde vaak problemen op, waardoor hij erg inventief moest zijn om dingen voor elkaar te krijgen. Hans heeft er wel erg veel van geleerd. Het team computercriminaliteit werd gezien als de computerdeskundigen, maar zij voelden zich niet altijd zo door alle verschillende computers die allemaal verschillende software hadden en verschillend werkten.

Hans Heins: "Een heel team van rechercheurs zat op ons te wachten, omdat wij bij een huiszoeking de computer moesten onderzoeken. Toen we binnenkwamen werd gezegd: aha, daar zijn de deskundigen. Op een bureau stond een strak vormgegeven zwarte computer. Ik had alles bij de hand voor onderzoek van de computer, maar het diskette station kon ik niet vinden. Waarschijnlijk zat dit verborgen achter het grote zwarte voorfront, wat bij het aanzetten van de pc zou opklappen. Het duurde even voordat ik de aan/uit knop gevonden had: deze was geplaatst in de voet van de pc".

Zij gingen op zoek naar software om een image copy naar de tape te maken en waarmee ook op te starten was. Zij dachten dit te vinden in Snapback, waarmee het backupen van schijf naar schijf mogelijk was. Backupen naar tape bleek niet de beste, maar wel de goedkoopste oplossing te zijn, een tape was maar op korte termijn betrouwbaar en bovendien hadden zij niet genoeg tapes.
Na 1 jaar gingen ze over op het kopiëren naar harde schijf. Het onderzoeken van een computersysteem werd gedaan met behulp van diskedit, wat enorm tijdrovend was aangezien er maar een zoekopdracht tegelijk uitgevoerd kon worden. Daarna kwam disksearch; hiermee konden max. 128 woorden tegelijk gezocht worden, maar dit nam nog steeds erg veel tijd in beslag en was lastig.

Ontdekking EnCase

Van de vijf jaar dat Hans Heins bij het team computercriminaliteit Haaglanden werkte gaf hij 4 jaar opleiding voor taak-accent-houders. Twee van zijn collega's gingen naar Amerika voor de beurs Export Witness in Amerika, dit was begin 1998. Zij brachten EnCase mee naar Nederland om nader te bekijken en zij kwamen gezamenlijk al snel tot de conclusie dat EnCase de tool is voor digitaal rechercheren en om te leren aan de taak accent houders. Hans is toen naar de cursus van EnCase versie 1 bij Guidance (de leverancier van EnCase) in Amerika gegaan. Ondertussen is hij al 3 keer in Amerika geweest. Naast EnCase heeft hij niet veel andere software nodig voor het digitaal rechercheren, wel maakt hij soms gebruik van Snapback, Ghost en ilook. Het laatste gebruikt hij om dingen uit te proberen.

Hans Heins tijdens het Digitaal Rechercheren

EnCase voor beginners

Op de vraag of Hans een goede raad heeft voor mensen die net begonnen zijn met EnCase geeft Hans het advies om veel te oefenen met data die zelf gecreëerd is. Probeer deze data terug te vinden en zichtbaar te maken. Doe eens een groot onderzoek en maak daarvan een draaiboek, formatteer de schijf daarna en probeer alles weer terug te vinden en controleer of dit klopt met je script. Kopieer bijvoorbeeld alle temp files naar een diskette en onderzoek ze daarna, tijdelijke bestanden zijn heel goed bij het onderzoeken van bestanden. Aldoende leert men.

Cursus EnCase

Hans geeft op het LSOP de B.D.R. (Basiscursus Digitaal Rechercheren), tijdens de cursus die in totaal drie weken duurt, wordt heel diep ingegaan op de materie. De cursisten leren eerst omgaan met de schijven, hardware, wetgeving, getallen (binair en hexadecimaal) en doorzoeking. Eerst wordt handmatig gezocht op schijven en pas in de laatste week wordt overgegaan op EnCase.
Bij DataExpert worden drie verschillende cursussen EnCase gegeven:

- 2-daagse EnCase Rechercheurscursus
- 5-daagse EnCase Uitgebreide Cursus
- 2-daagse EnCase 3 Upgrade Cursus

Deze cursussen gaan met name over het bedienen van het programma.

EnCase voor gevorderden
De doorgewinterde gebruikers moeten de scripts niet onderwaarderen. Een goede tip is om bij het zoeken naar bewijs zoveel mogelijk gebruik te maken van automatische recovery onder folders..Hans raadt ook aan te zoeken naar subdirectories, omdat dan alle bestanden te vinden zijn. Ook is het verstandig om achteraf te compressen. Hans geeft als tip standaard cases te maken om daarin alle woorden die met bijvoorbeeld drugs te maken hebben op te slaan.

Gebruik EnCase in het bedrijfsleven
Hans Heins: "In verband met het toenemende aantal computers worden steeds meer dingen gedaan die nadellig zijn voor het bedrijf. Het bedrijf wil daarvan niet altijd aangifte doen, daarom is het belangrijk dat er een expertise-afdeling binnen dat bedrijf komt, die het onderzoek professioneel aanpakt. Voor onderzoek moet een goede tool gebruikt worden, EnCase heeft ons al laten zien dat het voor dergelijke onderzoeken de goede tool is".

Nieuwe versie EnCase
Onlangs is EnCase versie 3 uitgeleverd. Bij met name bijzondere besturingssystemen geeft versie 3 veel meer mogelijkheden.
Daarnaast is het een groot voordeel dat het nu mogelijk is een backup te maken via een netwerkkabel, wat veel sneller is en weer meer mogelijkheden biedt. Ook de reportfunctie is uitgebreider: in versie 2 moest iedere bookmark apart van commentaar voorzien worden, nu kunnen bijvoorbeeld 120 items geselecteerd worden en in een keer van commentaar voorzien worden. Tijdens het geven van een zoekopdracht is het tevens mogelijk om aan te geven op wat voor een manier je je resultaat wilt door dit aan te geven in de header van het bestand.

Hans is erg enthousiast over de capaciteiten van EnCase, maar geeft toe dat de functionaliteiten soms helaas iets minder zijn. Hij doet hiermee op het soms vastlopen van het programma, wat volgens hem door de dynamiek van het programma komt.
Hans Heins: "De makers van EnCase luisteren goed naar de wensen van de gebruikers, waardoor het programma ontzettend dynamisch wordt. De ideeen worden omgezet in daden. Het is heel belangrijk dat een dergelijk programma vaak geupdate wordt, met als risico dat er soms een bug optreedt. Mensen onderschatten EnCase vaak: alles is te zien inclusief de gewiste bestanden. Mensen raken enthousiaster naarmate ze EnCase langer gebruiken".

Specifieke wensen van Hans

Op de vraag wat voor een specifieke wensen Hans nog heeft met betrekking tot de nieuwe versie EnCase, moet hij lang nadenken: *"Er kan al zoveel in EnCase".*
Hans wenst een ander soort tijdlijn, omdat de chronologische volgorde wat er op een pc gebeurt niet te krijgen is. Verder zou hij graag willen dat Guidence zelf scripts levert. Guidence verwacht dat de gebruikers zelf met scripts komen, wat tot op heden minimaal gebeurt. Op de website van Guidance is hier weinig van te vinden, wat Hans bereurt omdat de kracht van het programma daardoor veel groter zou worden.