

HC 5, 05-03-2019, Digitale sporen

Sporen die je achterlaat op je eigen PC

Je computer houdt 'onder water' alles bij wat je doet. Alles wordt in zogenaamde **logbestanden** opgeslagen. Zo kun je die informatie ook terug halen. Het operating system houdt deze logbestanden bij. Verder houdt het operating system nog bij:

- Metadata van/in bestanden.
- Niet echt verwijderde data op harde schijf.
- Bestanden zelf.
- De WiFi netwerken waarmee je ooit verbonden bent geweest.

Als je je laptop aan iemand anders zou geven, kan diegene precies zien met welke netwerken jij ooit verbonden bent geweest. Iedere applicatie zelf houdt ook best veel gegevens bij, zoals:

- Contactenlijst.
- Bezochte websites (browser history), dit kan je ook weer terug zien.
- Verzonden/ontvangen e-mails.
- Recent geopende bestanden (bestand waarin je gisteren hebt gewerkt in word kun je makkelijk weer openen).
- Afspraken in je agenda.
- Berichten.
- Wie wanneer heeft gebeld.

Dit soort gegevens zijn erg interessant voor de politie met betrekking tot opsporing. De politie mag een verdachte dwingen om zijn smartphone te ontgrendelen door onder dwang de duim van de verdachte op de identity sensor van de telefoon te plaatsen.

Via netwerkverbindingen

Netwerkverbindingen laten ook allerlei sporen achter. Een van de sporen is via de MAC adressen. Ieder apparaat heeft zowel een IP-adres als een MAC adres (uniek hardwareadres voor de directe verbinding tussen jouw computer en de router). Denk hierbij aan WiFi of bluetooth. Als je je telefoon aan hebt en je bent verbonden met de WiFi, dan wordt het MAC-adres van jouw telefoon constant uitgezonden. De VID gebruikt al jaren de MAC-adressen om de verkeersdrukte te meten.

Iedere keer dat jij probeert verbinding te maken met een draadloos netwerk, jouw telefoon een aantal bij hem bekende netwerken uitzendt. Dit doet hij om de kijken of deze in de buurt zijn, zodat daar mogelijk verbinding mee kan worden gemaakt. Ook worden de WiFi netwerken waarmee je ooit verbonden bent geweest lokaal opgeslagen.

Als je verbinding maakt met een onbeveiligd netwerk (free wifi) en bepaalde data verstuurt dan is het makkelijk voor anderen om hierbij te komen.

Sporen achtergelaten door mobiele telefonie

Als je met iemand belt, kan er enkel verbinding tot stand komen als de telefoonmaatschappij weet waar je bent (met welke telefoonmast sta je in verbinding). Als je een gesprek voert, worden de tijd, de duur, het gebelde nummer en je locatie opgeslagen om de hoogte van de abbonement te bepalen. Hetzelfde geldt voor SMS. Zo'n telefoonmast is geen specifieke locatie, dus daarmee kan niet precies worden vastgelegd waar je bent (in het harmoniegebouw of in het academiegebouw). Veel telefoonmaatschappijen bepalen je locatie door middel van een zogenaamde driehoeksmeting. Dat wil zeggen dat je telefoon in verbinding staat met één telefoonmast, maar ook al twee anderen detecteert en ziet hoe ver deze van de telefoon afstaan. Op die manier kan de precieze locatie worden bepaald. Die vorm van locatiebepaling willen ze ook invoeren bij de meldkamer van 112.

Sporen achtergelaten door het Internet

IP pakketten zijn briefkaarten en de data en het IP adres zijn in principe zichtbaar. Je IP adres is te herleiden tot een fysieke locatie (geolocation). Als je iemands IP adres hebt, kun je dit opvragen.

Bedrijven als Google en Amazone gebruiken dat. Door te kijken naar het poortnummer in die pakketjes kun je ook zien welke diensten diegene gebruikt (e-mail, webverkeer).

Wet bewaarplicht telecomgegevens

Deze wet is in 2014 ongeldig verklaard. Deze wet verplichtte aanbieders van openbare elektronische communicatienetwerken en aanbieders van openbare elektronische communicatiediensten tot het bewaren van:

- Telefoonnummers, namen en adressen van de betrokken abonnees etc.
- Datum ,tijdstip en e-mailadres van gebruiker.
- Datum en tijdstip van log-in en log-off en het IP-adres van de gebruiker.

Deze informatie kon gebruikt worden voor opsporing. Daarvan werd gezegd dat het niet proportioneel is om zoveel informatie te verzamelen van zoveel mensen.

→WIV (Wet op de Inlichtingen- en veiligheidsdiensten kwam hiervoor in de plaats).

Op het web

Om te begrijpen waarom cookies nodig zijn, is het van belang om te weten hoe het World Wide Web werkt. Als je een webpagina ophaalt, maakt je browser contact met de webserver van de pagina waar je heen wil, die vervolgens de informatie terugstuurt. Dit geldt ook voor iedere, aparte afbeelding op die pagina.

Het web is stateless

Het web houdt geen toestand bij. Dat wil zeggen dat ieder verzoek naar een website, los staat van alle andere verzoeken. Ook bij iedere afbeelding staan die verzoeken los van elkaar, daarvan kan de webserver niet zien dat het om dezelfde browser gaat. Een nadeel is als je bezoekers wil kunnen herkennen. Bijvoorbeeld als je inlogt op facebook, dan moet hij kunnen herkennen bij het ophalen van facebookpagina's dat jij het bent. Dit geldt ook voor het digitale winkelwagentje dat bijhoudt wat je mogelijk wil kopen. De webserver moet kunnen zien dat het hierbij telkens om dezelfde persoon gaat.

De oplossing: cookies

Een cookie is een combinatie van een naam + een waarde op te laten slaan in de browser. Die cookies zijn specifiek voor één website. De eerste keer dat je een website bezoekt, krijg je één of meer cookies van die website (bijvoorbeeld: language = dutch). Je browser slaat die op en de volgende keer dat je diezelfde website bezoekt, stuurt je browser alle cookies voor die website mee met ieder verzoek voor een pagina. In dit geval zou de pagina dan dus in het Nederlands worden getoond. Soms krijg je ook nieuwe of aangepaste cookies. Met een specifieke cookie al 'USERID = jhh' kun je alle items die je wil kopen in mijn winkelmandje plaatsen.

Iedere keer dat je op een link klikt of een plaatje voor een webpagina wordt opgehaald, dan wordt de URL (het webadres) van die pagina meegestuurd waar de link of het plaatje in staat. Dat betekent dat de webserver waar het plaatje of de link staat, de webserver waar de link naar verwijst weet waar dit verzoek vandaan komt. Als nu.nl plaatjes op de webpagina bevat van doubleclick, dan wordt bij het ophalen van het plaatje niet alleen www.nu.nl opgestuurd, maar ook alle cookies. Vanaf dat moment wordt die cookie (web bug) telkens opgestuurd als je een plaatje ophaalt van doubleclick. Op basis daarvan kunnen websites je profileren.