

Security.nl onderzoek tweedehands harde schijven



“Digitale verledens open en bloot op Marktplaats.nl”

Inhoudsopgave

Inleiding.....	3
Onderzoeksmethode.....	3
Gereedschap.....	3
Zoekcriteria.....	4
Extensies.....	4
Resultaten	4
Misbruik.....	5
Oplossing	5
Conclusie	5
Bijlage A: Werken met Helix.....	6

Inleiding

Dagelijks verkopen vele duizenden mensen en bedrijven hun oude computers en harde schijven, geven die weg of zetten die bij het grof vuil. De meesten beseffen niet dat de informatie op de harde schijf vaak eenvoudig is terug te halen, ook al heeft men die geformatteerd. Daarnaast zijn er ook nog altijd mensen die er helemaal niet aan denken om hun digitale verleden van de harde schijf te verwijderen.

Security.nl liet twee studenten van het Albeda College te Rotterdam twintig op Marktplaats gekocht harde schijven onderzoeken. Hierop werd allerlei persoonlijke informatie aangetroffen, zoals incasso machtigingen, medische gegevens, belastingdocumenten, bedrijfsinformatie, C.V.'s, een dagboek, sollicitatiebrieven, inkooporders, faxen, e-mails en veel porno en privé foto's.

Bij de aanschaf werd specifiek gekeken of de aanbieder een particulier was. Eén van de verkopers merkte zelfs op dat de schijf eerst door ons geformatteerd moest worden, "aangezien het besturingssysteem en alles er nog op staat."

Onderzoeksmethode

Voor het uitvoeren van het onderzoek was de belangrijkste vereiste dat het met gratis software moest gebeuren die iedereen kan gebruiken. Dit laat zien dat het terughalen van vertrouwelijke informatie niet alleen aan forensische onderzoekers is voorbehouden, maar elke computergebruiker dit kan doen.

Om te voorkomen dat er tijdens het onderzoek belangrijke gegevens verloren gingen werd er van alle harde schijven eerst een image gemaakt: een kopie op een andere harde schijf, die voorkomt dat bestanden op de originele harde schijf aangepast worden of beschadigd raken. Dit werd gedaan met het programma Adepto, een onderdeel van de Helix toolkit. Dit programma is voor forensische onderzoeken gemaakt en werkt vanaf een opstartbare CD-rom. De CD zorgt ervoor dat de data alleen van de harde schijf is te lezen en er niet naar toe geschreven kan worden.

Het terughalen van de verwijderde- en geformatteerde data, als dat al nodig was, werd gedaan met Foremost. Het programma is snel, kent geen beperkingen en is bovendien gratis. Dit pakket draait in een Linux omgeving. Het programma zoekt bestanden aan de hand van headers en probeert zodoende beschadigde bestanden bij elkaar te zoeken en te herstellen. Dit wordt "datacarving" genoemd. De onderzoekers hebben via Foremost de verschillende soorten bestanden gesorteerd en bekeken.

Gereedschap

Forensisch onderzoek verrichten op opslagmedia kan zowel onder Linux als Windows. Met name voor de minder ervaren gebruikers biedt de Forensic Toolkit uitkomst. Onder Linux is er het programma Sleuthkit/Autopsy of PTK. Deze programma's kunnen diverse image bestanden openen en vervolgens hier sectie op verrichten. Alle genoemde programma's hebben "datacarving" als functie. Er is verder geen speciale hardware vereist.

Zoekcriteria

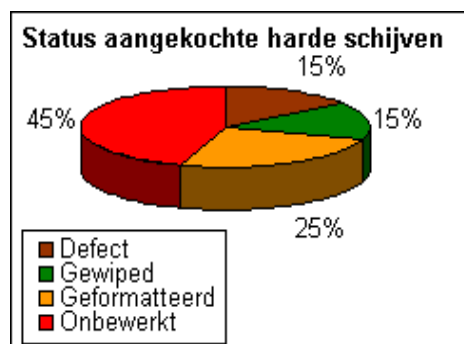
Er werd gezocht naar persoonlijke documenten en persoonlijke foto's/filmpjes. Het kan namelijk een gevaar voor de privacy van iemand opleveren, als er bijv. een adres gevonden wordt, of nog erger, een PIN-code. Er moet dan gedacht worden aan bijvoorbeeld stalking, fraude en andere criminele activiteiten.

Extensies

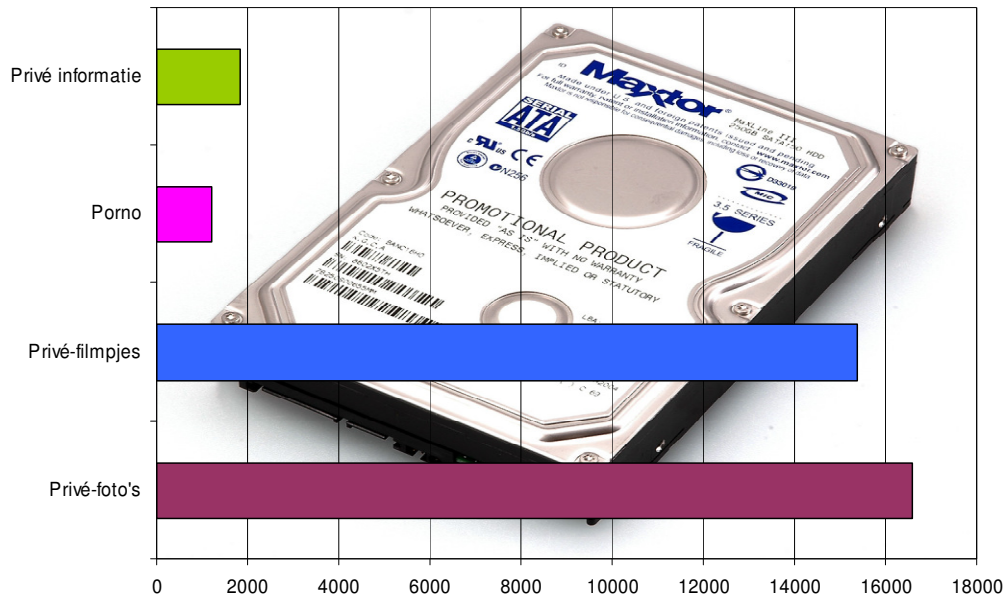
Foto's	Video	Documenten
*.JPG	*.AVI	*.DOC
*.PNG	*.MOV	*.PDF
*.GIF	*.WMV	*.TXT
*.BMP	*.MPEG	

Resultaten

In totaal zijn er twintig harde schijven onderzocht, waarop in totaal 795.005 bestanden achterhaald werden. Drie schijven bleken defect en daardoor niet meer te onderzoeken. Van de overige zeventien harde schijven waren er drie op een adequate manier gewist, zodat er geen data te herstellen was. In totaal bevatten de overige 14 harde schijven relevante informatie. Vijf harde schijven waren geformatteerd, maar dit was niet voldoende, aangezien alle gegevens te achterhalen waren. Bij negen schijven was er niet eens de moeite gedaan om gegevens te wissen.



De aangetroffen bestanden bestonden voornamelijk uit privé foto's (16.601), filmpjes (15.390) en porno (1.221). Daarnaast werd er ook veel vertrouwelijke data aangetroffen zoals een dagboek, inkooporders, e-mails, faxen, belastingdocumenten, rekeningnummers, een dreigbrief aangaande een persoonlijke lening, een gescande identiteitskaart, e-mailadressen, ledenlijsten van verenigingen, telefoonnummers, bedrijfsgegevens, logbestanden van MSN-gesprekken en sollicitatiebrieven met volledige C.V.'s. Op alle 14 harde schijven met informatie werden gevoelige gegevens gevonden. Bij elkaar 1.839 bestanden. De pornografische filmpjes en foto's stonden op zeven harde schijven.



Overzicht van aantal en soort bestanden

Misbruik

Afhankelijk van de gevonden informatie kunnen criminelen mensen afpersen, identiteitsfraude plegen of toegang tot persoonlijke gegevens krijgen, zoals wachtwoorden voor e-mail accounts of websites.

Oplossing

De hierboven beschreven problematiek kent twee oorzaken. Consumenten zijn onbekend met de gevaren of weten niet hoe ze een harde schijf op een adequate manier kunnen wissen. Om gebruikers bij dit proces te helpen heeft Security.nl een instructievideo gemaakt die in nog geen 6 minuten stap voor stap uitlegt hoe men aanwezige bestanden permanent kan wissen. Wie besluit zijn oude computer of harde schijf weg te doen, wordt dringend aangeraden eerst de volgende video te bekijken <http://www.security.nl/hdwissen>

Deze vide demonstreert het gebruik van Darik's Boot And Nuke, zogeheten "Wiping software". Wipen is niet hetzelfde als formatteren, omdat bij formatteren alleen de locatie van het bestand wordt verwijderd. Omdat de locatie niet meer bekend is, kan men het bestand ook niet meer zien, maar het bestand staat nog wel op de harde schijf. Door de harde schijf te wipen wordt alle data van de harde schijf verwijderd en overschreven en is daardoor niet meer terug te halen.

Conclusie

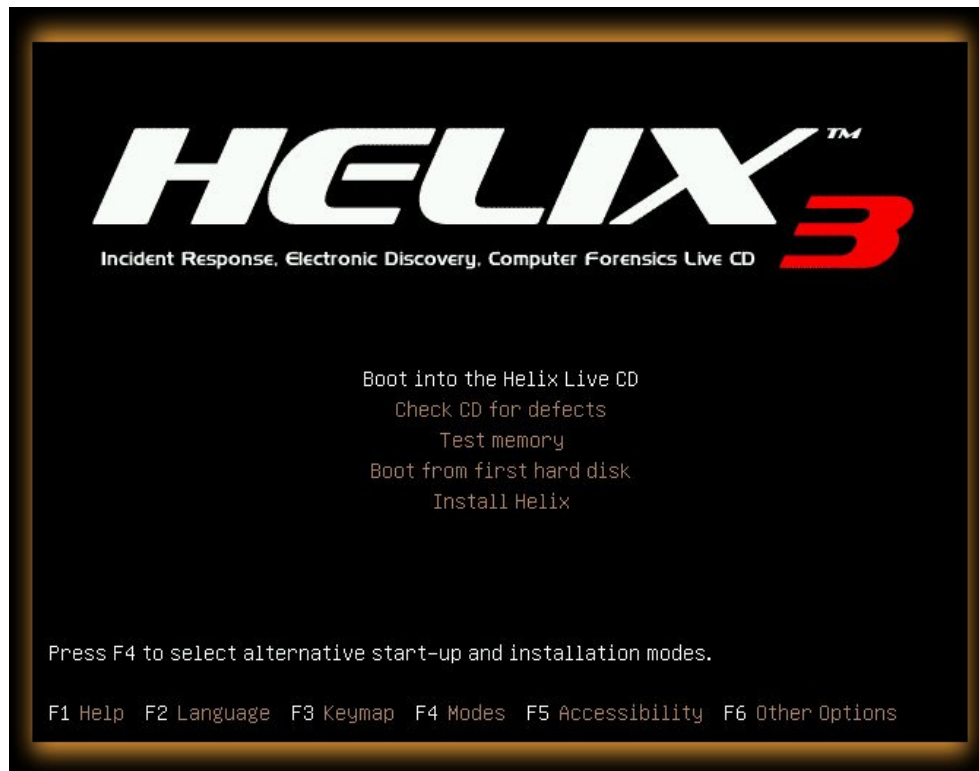
Ondanks alle verhalen over gegevens die op straat belanden of criminelen die hier misbruik van maken, blijkt dat consumenten nog altijd zeer onzorgvuldig met hun persoonlijke informatie omgaan. Er valt daarom nog een enorme inhaalslag te maken wat betreft bewustzijn en voorlichting.

Door dit onderzoek en de bijbehorende instructievideo hopen we dat consumenten zich bewust worden dat harde schijven persoonlijke informatie bevatten en dat iedereen

adequaat een schijf kan wissen. Tenslotte is voorkomen beter dan genezen, zeker als het om gevoelige informatie gaat.

Bijlage A: Werken met Helix

Wanneer men de Helix live CD start krijgt men het volgende scherm te zien:



Mocht dit niet het geval zijn dan zou de kans groot zijn dat men het volgende scherm ziet:



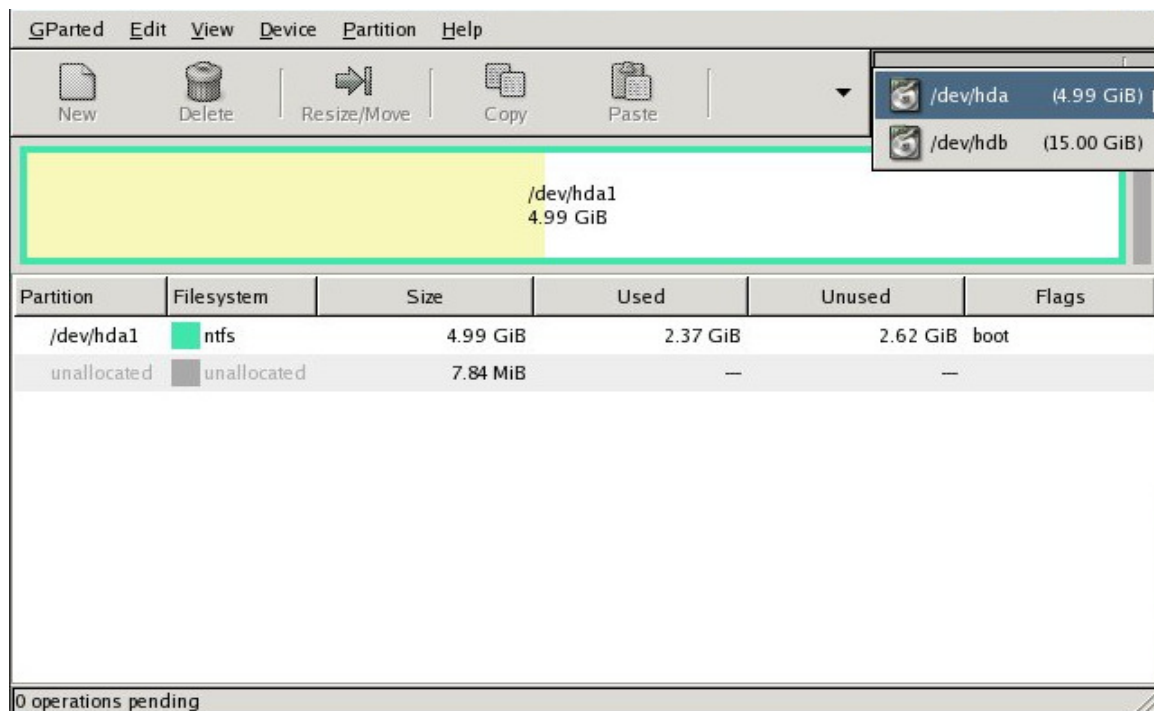
In beide gevallen kiest u voor de bovenste optie, in optie 1 is dit “**Boot into the Helix Live CD**” in optie 2 is dit “**GUI**”. Helix zal nu worden opgestart.

Wanneer men in de Helix omgeving is aangekomen gaat men naar **Applications** en vervolgens naar **Accessories**. In dit menu ziet men **Terminal** staan, men klikt deze aan.

Er verschijnt vervolgens een wit scherm met zwarte letters. U typt hier het volgende in:”

sudo parted

Men zal een vergelijkbaar beeld te zien krijgen als de afbeelding hier onder:



Zoals u hier boven kunt zien, ziet u een balk wat de harde schijf moet voorstellen van 4,99 GB. Rechts boven in ziet u nog een andere harde schijf van 15 GB. Voor de grote van de harde schijf ziet u */dev/hda* of */dev/hdb* staan. Dit pad is van groot belang voor het maken van een image van de harde schijf.

In deze situatie wil men een Image maken van de 4,99 GB harde schijf en weg te schrijven op de 15 GB schijf. Om dit te kunnen doen moet de harde schijf van 15 GB wel beschrijfbaar zijn, standaard zorgt Helix ervoor dat dit niet kan, zodat men gewoon de harde schijven kan openen zonder sporen achter te laten. Om te kunnen veranderen zal men weer eerst een Terminal moeten openen, men deed dit door het volgende te doen:

Men gaat naar **Applications > Accessories > Terminal** en klikt deze aan. Er zal weer een wit scherm verschijnen met witte letters. Met typt hier het volgende in om de 15 GB beschrijfbaar te maken:

Mocht de schijf een NTFS schijf zijn, dan moet men het volgende commando invoeren in plaats van de voorgaande tekst.

```
sudo mount.ntfs-3g /dev/hdb /media/hdb
```

Men zal zien dat in de tekst **hdb** staat, dit is het verwijzingspad van de harde schijf van 15 GB. De schijf is nu beschrijfbaar en men kan nu de image wegschrijven op deze schijf. Hier onder kunt u zien hoe men dit doet.

Voor het maken en het wegschrijven van de Image gebruikt men Adepto. U kunt dit programma vinden als u naar **Applications** gaat en vervolgens naar **Forensics & IR** en dan staat boven aan **Adepto**. Als u deze optie aanklikt start het programma op en zult het eerste tabblad zien, **Start**. Hier voert u een naam in. Wanneer men een naam heeft ingevoerd wordt men naar het volgende tabblad geleid, dit is het tabblad **Device info**, waar u een harde schijf/partitie moet selecteren. Van deze harde schijf/partitie gaat Adepto een image maken.

Wanneer men dit heeft gedaan kunt u naar het volgende tabblad. Dit is het tabblad Acquire. Dit tabblad word verdeeld in de volgende groepen:

Source information

Source device Dit is het punt waar Adepto een image van gaat maken
Image name Hier kunt u de image een naam geven.

Destination information

Mount point Dit is de locatie waar u de harde schijf naar toe schrijft

Options

MD5 Hiermee word geverifieerd na het maken van de image, of deze gelijk is aan het origineel
DCFLDD Dit is een optie die standaard ingesteld staat, met behulp van dit programma word de image gemaakt.

Wanneer men deze velden heeft ingevuld en de juiste vakjes heeft aangevinkt kan men beginnen met het maken van een Image, dit doet men door **Start...** te selecteren. Als de Image klaar is, wordt de MD5 waarde geverifieerd met de waarde van de harde schijf. Adepto geeft aan het eind van het maken van een image aan of dit is gelukt.

Software links

<http://foremost.sourceforge.net/>
<http://helix.e-fense.com/Download.html>
<http://www.security.nl/hdwissen>