

1 Doel

Deze procedure beschrijft het onderzoek "veiligstellen van een fysieke gegevensdrager" en focust zich in het bijzonder op het veiligstellen van een harde schijf. Het resultaat van dit onderzoek kan dienen als onderzoeksmateriaal in bijvoorbeeld een data-analyseonderzoek.

2 Principe

Gedurende het onderzoek wordt een één-op-één-kopie of een zo compleet mogelijke deekopie gemaakt van de inhoud van een stuk van overtuiging naar een ander opslagmedium. Hiervoor wordt gebruik gemaakt van speciaal daarvoor ontwikkelde hard- en software. Tijdens iedere stap in het proces wordt de integriteit van de data gewaarborgd door middel van het berekenen van bestandskenmerken.

3 Toepassingsgebied

De procedure wordt toegepast op alle opslagmedia met standaard (fysiek ontkoppelbare) interfaces die gebruikelijk zijn in een PC-omgeving, zoals harde schijven, solid state harde schijven, geheugenkaarten, et cetera.

Opslagmedia die geen ontkoppelbare interface hebben (maar bijvoorbeeld gesoldeerd zijn) vallen buiten de scope van dit document.

4 Werkwijze/uitvoering

Bij aanvang van de procedure.

Bij nieuwe aanvraag, zorg voor de volgende zaken:

- Zo volledig mogelijk ingevuld aanvraagformulier.
- Toestemming mogelijk destructief onderzoek.
- Verwijs voor vervoer en verpakking SVO's naar FT-norm 1300.02.
- Vraag proces verbaal van uitgevoerde handelingen.

Leg de volgende zaken klaar bij aanvang van het onderzoek:

- Waarnemingsformulieren passend bij SVO (liggen in de postvakjes naast de videomonitor).
- (Bij harde schijf) flowchart hard disk repair (Zie documenten onder versiebeheer DT).

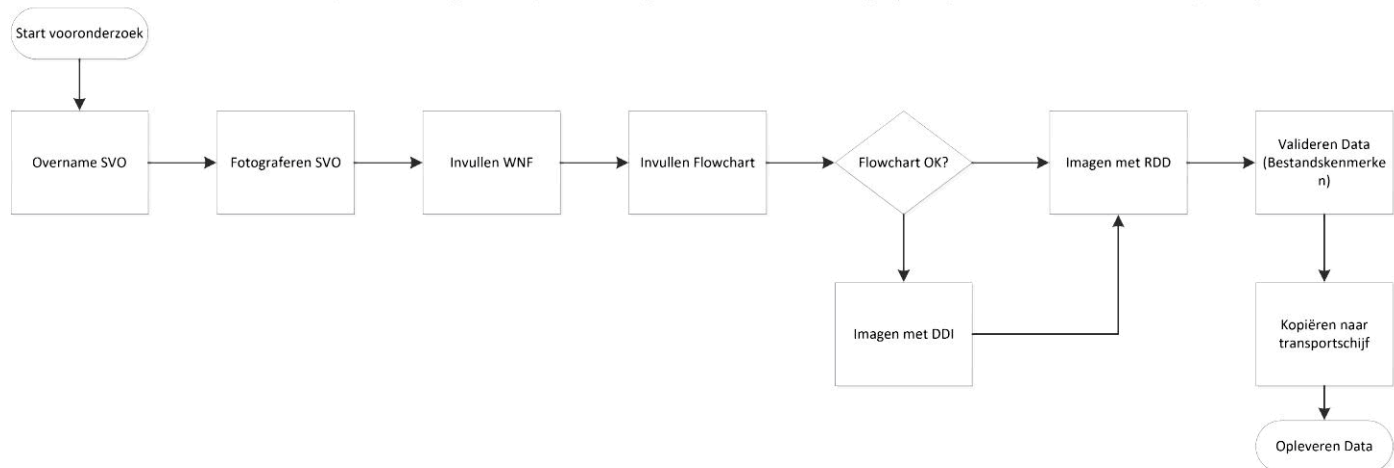
Procedure fotograferen en noteren

- Zorg dat de labtafel schoon en leeg is.
- Vul waarnemingsformulier in.
- Fotografeer verpakking SVO van alle zijdes, leg (indien van nut) een liniaal bij het object, zorg dat zaaknummers en SIN goed te zien zijn.
- Neem SVO uit verpakking, maak indien nodig gebruik van persoonlijke beschermingsmiddelen (handschoenen, labjas, mondkapje, afzuigingsinstallatie).
- Fotografeer SVO van alle zijdes, maak detailfoto's van bijzonderheden en eventuele schades. Noteer deze ook op het waarnemingsformulier.
- Zorg dat SIN en zaaknummer bij het fotograferen in beeld zijn.
- Gebruik zoveel mogelijk dezelfde camera voor hetzelfde SVO.
- Bekijk na het nemen van een foto of deze scherp is.
- Voeg SINS toe aan alle gegevensdragers aanwezig in het SVO.

FDT - veiligstellen fysieke gegevensdragers

Procedure onderzoek aan harde schijven

- Volg dit stappendiagram voor een onderzoek aan een harde schijf:
- Gedurende het onderzoek worden alle delen van de te onderzoeken harde schijf gelabeld met SIN nummer (met labelprinter). Schroefjes worden in een gripzakje met SIN-nummer gestopt zodat



duidelijk is welke schroefjes bij welke harde schijf horen.

Voor maatwerk (DTE201) volgt een onderzoeksplan, met het uitgevoerde onderzoek (DTE001) als uitgangspunt.

Controle/vrijgave tussenresultaten

Tussentijdse resultaten worden gecontroleerd door middel van controle bestandskenmerken, berekend over iedere stap in het proces.. Indien bij het kopiëren van SVO's geen leesfouten optreden worden bestandskenmerken m.b.v. een writeblocker direct over de inhoud van het SVO berekend.

Berekenen bestandskenmerken in het proces:

- Berekende bestandskenmerken tijdens veiligstellen met RDD (MD5 en SHA-1, afhankelijk van RDD-versie ook SHA256)
- (indien geen RDD) DDI-Doelschijf (SHA256)
- Gemaakte één-op-één-kopie van de doelschijf (SHA256)
- Na kopiëren één-op-één-kopie naar transportschijf (SHA256)
- Registratie van bestandskenmerken, uitgevoerde commando's en uitkomsten op waarnemingsformulieren
- Opleveren SIN-formulieren bij één-op-één kopieën met bijbehorende MD5, SHA-1- en SHA256-bestandskenmerken volgens template (zie documenten onder versiebeheer DT)

Controle/vrijgave apparatuur

Controle apparatuur voor ingebruikname:

Ace Laboratories

PC3000 (Alle systemen)

Voor ingebruikname getest op:

- Doorvoersnelheid bus
- Mogelijkheid tot sturen fabriekscommando's naar aangesloten disk
- Werking seriële poort

Bij tussentijdse reguliere updates wordt alleen de werking van de software getest.

Logging in logboek, aanwezig in de computerkast van het PC-3000 hostsysteem:

FDT - veiligstellen fysieke gegevensdragers

- Specificaties hostmachine
- Opgetreden fouten/problemen
- Uitgerolde updates (Inclusief notatie versienummers en buildnummers)
- Geïnstalleerde software (inclusief notatie versienummers en buildnummers)
- Tussentijds geïnstalleerde hardware

Alle logboekregels zijn voorzien van datum + paraaf onderzoeker.

Deepspaar Data Recovery Systems

Deepspaar Disk Imager (Beide systemen)

Voor ingebruikname getest met DDI Testdisk (te vinden op systeemkast DDI3) en doelschijf (Voorzien van DEVTEST-patroon)

Na test hashwaardes berekenen van doelschijf en bronschijf, indien identiek vrijgave voor gebruik.

Deze test wordt ook gebruikt bij tussentijdse updates.

Logging in logboek, aanwezig in de computerkast van het DDI-hostsysteem:

- Specificaties hostmachine
- Opgetreden fouten/problemen
- Uitgerolde updates (Inclusief notatie versienummers en buildnummers)
- Geïnstalleerde hard- en software (inclusief notatie versienummers en buildnummers)

Alle logboekregels zijn voorzien van datum + paraaf onderzoeker.

Imagingwerkplekken

Logging in logboek, aanwezig bovenop kast systeem of muur achter systeem:

- Specificaties hostmachine
- Opgetreden fouten/problemen
- Uitgerolde updates (Inclusief notatie versienummers en buildnummers)
- Geïnstalleerde software (inclusief notatie versienummers en buildnummers)
- Tussentijds geïnstalleerde hardware

Alle logboekregels zijn voorzien van datum + paraaf onderzoeker.

Minder vaak gebruikte systemen (bv. **busdoctor host** en **microscoop PC**) zijn eveneens voorzien van een logboek, volgens hetzelfde formaat.

5 Wijzigingen ten opzichte van vorige versie

Versie	Datum	Auteur	Opmerking
1.0	09-01-2017	5.1.2e	Initiële versie