ENCRYPTIE VOOR ONDERZOEKERS

UNIVERSITEIT GENT

INHOUD

Dit document kwam tot stand in samenwerking met volgende diensten:

- de Directie Onderzoeksaangelegenheden, Afdeling Universiteitsbibliotheek - Data Steward Team
- de Directie Onderzoeksaangelegenheden, Afdeling Onderzoekscoördinatie
- de Directie Informatie- en Communicatietechnologie
- de Directie Bestuurszaken.

I. WAT IS ENCRYPTIE?

Encryptie (of versleuteling) is een methode waarbij data onleesbaar worden gemaakt door middel van bepaalde algoritmen. Deze algoritmen gebruiken een wachtwoord als basis om de data te versleutelen en om de versleutelde data te kunnen lezen moet je beschikken over dit wachtwoord.

Op deze manier wordt het voor derden onmogelijk om de versleutelde data in te kijken. Maar dit betekent ook dat wanneer je zelf niet langer over het wachtwoord beschikt, je de data niet meer kan openen.

De beveiliging valt of staat natuurlijk bij de keuze van een goed wachtwoord. Denk dus eerst goed na over het wachtwoord dat je zal gebruiken. Tips voor het creëren van een sterk wachtwoord zijn samen te vatten in volgende vuistregels: (1) hoe langer hoe beter (min. 10 karakters), (2) combineer zowel letters, cijfers als speciale tekens, (3) zorg dat je het wachtwoord kan onthouden (gebruik bijvoorbeeld een wachtwoordzin). Voor meer tips bij het kiezen van een sterk wachtwoord zie https://www.safeonweb.be/nl/gebruik-sterke-wachtwoorden.

Het is ook belangrijk te beseffen dat encryptie van data een goede back-up niet vervangt. Encryptie biedt geen bescherming tegen het (ongewild) verwijderen van data. Versleutelde data moeten dus nog steeds goed geback-upt worden.

II. WANNEER ENCRYPTEREN?

> Tip: Het is een beter om vertrouwelijke gegevens niet op een lokaal toestel (laptop, usb-stick, …) te bewaren, maar enkel op de centrale schrijfruimte die wordt beheerd door DICT. Indien dit niet kan, is het raadzaam om te encrypteren.

Wanneer je in het kader van je onderzoek vertrouwelijke[1] gegevens verzamelt en opslaat is het raadzaam om deze te encrypteren. Om te weten of encryptie nodig is moet je de afweging maken of er een verhoogd risico bestaat dat de data die je vertrouwelijk wil houden door onbevoegden zouden kunnen worden gelezen en wat de impact hiervan kan zijn (in een worst case scenario).

Een vuistregel kan zijn dat indien de gegevens de 'muren' van de UGent verlaten, er een verhoogd risico is. Wil je dus vertrouwelijke gegevens delen met anderen via de cloud, via filesender of via mail, dan dien je deze te encrypteren. Heb je vertrouwelijke gegevens op je laptop staan of op een extern medium dat je meeneemt naar huis (bv. USB-stick), dan is encryptie ook aangewezen. Wees je er ook van bewust dat wanneer je moet inloggen met een wachtwoord op je laptop, dit niet noodzakelijk betekent dat de gegevens op de laptop beschermd zijn tegen ongewenste blikken. Het inlogwachtwoord schermt de toegang tot jouw account af, maar maakt de gegevens die je hebt opgeslagen niet onleesbaar. Iemand die weet wat hij doet kan op die manier heel eenvoudig gegevens van je laptop halen. Dit kan enkel worden vermeden door het gebruik van encryptiesoftware zoals BitLocker (Windows) of FileVault2 (MacOS) (Zie ook Scenario 1 – Een volledige laptop encrypteren).

Wanneer de vertrouwelijke gegevens op een netwerkschijf van de UGent staan is het in principe niet nodig deze de encrypteren. Voor zeer gevoelige gegevens is het echter aan te raden extra veiligheidsmaatregelen te nemen en toch encryptie te gebruiken.

[1] Voor een classificatie van vertrouwelijke gegevens zie https://www.ugent.be/intranet/nl/op-het-werk/ict/informatieveiligheid/classificatie-data.pdf

III. HOE ENCRYPTEREN?

> Tip: Bewaar je vertrouwelijke gegevens op je UGent laptop? De gemakkelijkste manier om deze te beveiligen is versleutelen met BitLocker (windows).

Er bestaat een ruime keuze aan versleutelsoftware. Vooraleer een overzicht te geven is het belangrijk even in te gaan op de manier waarop deze programma's werken.

Volumes en containers

Simpel gesteld gebruiken gespecialiseerde softwarepakketten twee methodes om te versleutelen: containerencryptie en volume-encryptie.

Bij *containerencryptie* wordt er een soort container of doos gemaakt waarin de bestanden die je wil encrypteren worden geplaatst. Dit is vergelijkbaar met een zip-bestand. Deze doos wordt met een encryptiesleutel (bv. een wachtwoord) vergrendeld en onleesbaar gemaakt. Omdat deze "doos" in werkelijkheid niets anders is dan een bestand, heeft ze dan ook de eigenschappen van een gewoon bestand. Je kan het containerbestand verplaatsen (bv. van je schijf naar een usb-stick) en kopiëren, maar je kan het bestand ook gemakkelijk verwijderen. Dit laatste houdt vanzelfsprekend ook een gevaar in. Een goede back-up blijft dus belangrijk.

Bij *volume-encryptie* wordt het volledige medium waarop de data komen te staan versleuteld. In de praktijk gaat het dan meestal over een externe harde schijf, een USB-stick of de systeemschijf waarop je besturingssysteem staat. In technische termen worden dit vaak “volumes” genoemd, vandaar de naam volume-encryptie. Bij dit type van encryptie zijn de versleutelde bestanden vast verbonden aan het medium, aan de hardware. Dit is op het eerste zicht minder flexibel (je kan het versleuteld volume niet zomaar ergens heen kopiëren), maar het heeft ook voordelen. Zo is het gevaar dat je het volume per ongeluk verwijderd veel kleiner. Ook is dit een handiger manier om grote hoeveelheden data te versleutelen.

Naast gespecialiseerde versleutelsoftware zijn er ook andere manieren om te versleutelen. Sommige comprimeerprogramma's laten ook toe om een zip-bestand te encrypteren. Ook is het in de meeste office-pakketten mogelijk om een bestand met een wachtwoord te beveiligen en encrypteren.

Multiplatform?

Elk modern besturingssysteem beschikt over de nodige tools om encryptie uit te voeren. Deze zijn handig en werken goed zolang je zeker bent dat het versleutelde medium nooit op een ander besturingssysteem zal gebruikt worden. Met andere woorden, deze programma's werken niet platformonafhankelijk en zijn daarom niet aangewezen in een setting waar samenwerking en het delen van data belangrijk zijn.

In Tabel 1 en 2 wordt een vereenvoudigd overzicht gegeven van software om te encrypteren. De voorbeelden in Tabel 1 zijn programma's met als eerste en enige taak het encrypteren van data. De voorbeelden in Tabel 2 daarentegen zijn programma's zijn die encryptie voorzien naast hun andere primaire taak.

Tabel 1 - Gespecialiseerde encryptiesoftware

Programma	Encryptie van
Bitlocker (Windows)	Volume (systeemschijven en usb)
FileVault 2 (MacOS)	Volume (systeemschijven en usb)
VeraCrypt	Volume en container
Cryptomator	Container

Tabel 2 – Niet-gespecialiseerde software met encryptiefunctionaliteit

Programma	Encryptie van
7-Zip	Container
SPSS	Bestand
Office (Microsoft, Libre)	Bestand

De lijst is veel langer dan dit (voor een overzicht zie https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software).

Hardware oplossingen

Indien je vaak usb-sticks uitwisselt met vertrouwelijke informatie kan je ook exemplaren kopen met "ingebouwde" encryptie. Dit werkt goed, maar is relatief duur.

IV. SCENARIO'S

Omdat de keuze van het juiste versleutelingstool vaak afhangt van de situatie en het doel vertrekken we in deze how-to vanuit een aantal scenario's. Nadien volgen uitgewerkte voorbeelden per scenario.

Scenario 1 – Een volledige laptop encrypteren

Stel, je bewaart vertrouwelijke data op de harde schijf van je laptop die je overal meeneemt.

In dit scenario kan je het beste de systeemschijf waarop de data staan encrypteren. Hiervoor kan je de versleutelsoftware van je besturingssysteem gebruiken (BitLocker voor Windows, Filevault2 voor MacOS, dm-crypt voor linux).

Aan de slag!

Scenario 2 – Eén of enkele bestanden encrypteren

Stel, je wil 1 of enkele vertrouwelijke bestanden delen (via mail, filesender, cloud) met een collega.

Als de software waarmee je het bestand bewerkt encryptie voorziet, dan is het een goede keuze om dit te gebruiken. Het voordeel is dat je dan geen extra programma's nodig hebt. Zo bieden de meeste office-programma's (bv. Microsoft Office, LibreOffice), maar ook SPSS de mogelijkheid om bestanden te versleutelen met een wachtwoord.

Voorziet de software waarin je het bestand bewerkt geen encryptie of wil je snel enkele bestanden groeperen in een versleuteld geheel, dan kan je 7-zip gebruiken. 7-zip is compressiesoftware die ook toelaat om het zip-bestand dat je maakt te encrypteren. Het is bovendien vrij beschikbaar voor alle gangbare besturingssystemen (http://www.7-zip.org/) en wordt standaard geïnstalleerd op uitgerolde UGent-computers.

Het versleutelde zip-bestand kan je dan delen met je collega zoals je dat wil (bv. via mail, filesender, cloud). Natuurlijk moet je ook het wachtwoord delen met je collega. Een veilige manier om dit te doen is telefonisch of via een SMS.

Aan de slag!

Scenario 3 – Een projectfolder encrypteren

Stel, je wil dynamisch (samen)werken met vertrouwelijke data. Dit betekent dat je gemakkelijk bestanden wil kunnen toevoegen, bewerken en verwijderen binnen een beveiligde opslagplaats voor data. Voor dit scenario is het aangewezen om een 'encrypted file container' aan te maken met gespecialiseerde software.

In dit scenario kan je bijvoorbeeld VeraCrypt gebruiken. VeraCrypt is vrij beschikbaar voor alle gangbare besturingssystemen (https://VeraCrypt.codeplex.com/).

Een andere toepassing is Cryptomator (https://cryptomator.org/). Dit pakket heeft als bijkomend voordeel dat het geoptimaliseerd is om te gebruiken in combinatie met cloudopslag. Bovendien zijn er ook mobiele versies van de software beschikbaar voor het gebruik op je smartphone en tablet. De mobiele versies zijn niet gratis.

Aan de slag!

Scenario 4 – Externe devices encrypteren

Stel, je hebt een grote hoeveelheid data die je voor jezelf veilig wil bewaren op een externe harde schijf of usb-stick.

In dit scenario is het aangewezen om de volledige schijf te encrypteren met BitLocker (als je met Windows werkt) of Filevault2 (als je met MacOS werkt). Wil je de versleutelde externe harde schijf ook op andere besturingssystemen kunnen gebruiken dan dat van jou, dan kies je beter voor multiplatform software zoals VeraCrypt.

Belangrijk! Bij langdurige opslag is het belangrijk om het wachtwoord niet te vergeten. Gebruik een sterk[2] wachtwoord en bewaar het op een veilige plaats. Zorg er ook voor dat anderen die eventueel later over de data moeten kunnen beschikken (bv. je promotor) ook over het wachtwoord beschikken. Wachtwoorden kan je ook bewaren in een wachtwoordmanager zoals KeepassXC.

Aan de slag!

V. AAN DE SLAG

Scenario 1 – Volledige laptop encrypteren

Wanneer je op je laptop vertrouwelijke gegevens bewaart en je deze laptop ook buitenshuis (i.e. buiten de UGent) gebruikt, dan is het sterk aanbevolen om je de harddisk te encrypteren. Dit is in de meeste gevallen mogelijk met tools die worden meegeleverd met het besturingssysteem waarmee je werkt. Voor Windows is dit BitLocker en voor MacOS is dit FileVault2.

Encryptie van de systeemschijf in Windows met BitLocker

Vooraleer je aan de slag gaat, is het belangrijk volgende zaken te controleren.

- BitLocker is enkel beschikbaar voor de "professionele" edities van Windows (Enterprise, Ultimate). Voor laptops die zijn uitgerold binnen de UGent is dit normaal gezien geen probleem, maar voor laptops die zelf zijn aangekocht kan dit anders zijn omdat daar vaak de "lichtste" Home-editie op geïnstalleerd staat.
- Om je systeemschijf te encrypteren is het ook noodzakelijk dat je met een modern toestel werkt dat beschikt over een Trusted Platform Module (TPM). Dat is een speciale encryptiechip die vast in je laptop zit en die gebruikt wordt bij het versleutelen van je systeemschijf. Indien je geen TPM hebt, dan zal je hier melding van krijgen tijdens het activeren van BitLocker.

> Tip: Ga reeds bij de aankoop van je laptop na of je PC uitgerust is met een Trusted Platform Module, én zorg ervoor dat er een professionele versie van Windows op is uitgerold. Bij twijfel, contacteer de helpdesk van DICT.

[2] http://helpdesk.ugent.be/account/wachtwoord.php

Hoe je kan controleren of je een TPM-chip in je computer pc hebt vind je op volgende website: https://www.howtogeek.com/287737/how-to-check-if-your-computer-has-a-trusted-platform-module-tpm-chip/

Een goede handleiding over hoe je BitLocker moet instellen op een Windows PC vind je op volgende website: http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/

Voor de volledige, eerder technische uitleg kan je ook terecht op: https://technet.microsoft.com/en-us/library/c61f2a12-8ae6-4957-b031-97b4d762cf31

Encryptie van de systeemschijf in MacOS met FileVault 2

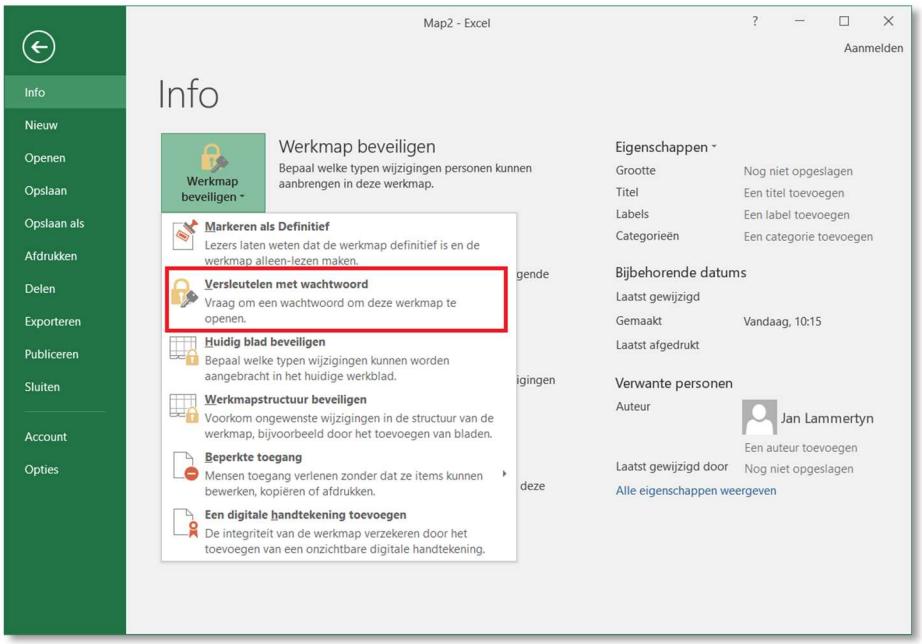
Op de website van Apple vind je een goede handleiding over het gebruik van FileVault 2 en het encrypteren van je systeemschijf: https://support.apple.com/en-us/HT204837

Scenario 2 – Eén of enkele bestanden encrypteren

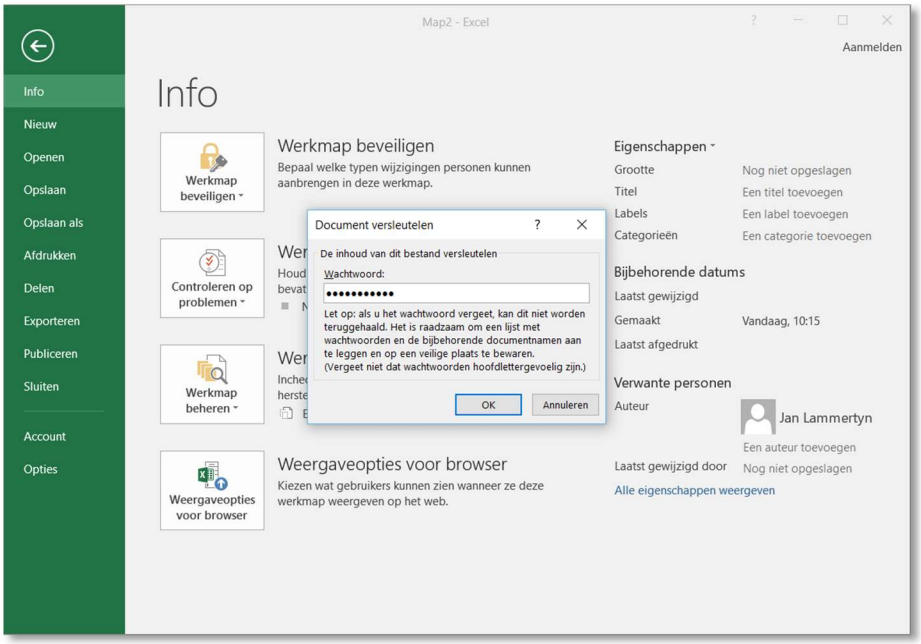
Als je snel één of enkele bestanden wil encrypteren omdat je ze bijvoorbeeld wil delen met een collega, dan kan je in sommige gevallen gebruik maken van de software waarmee je de data bewerkt (bv. SPSS). Heeft de software waarmee je de databestanden bewerkt deze mogelijkheid niet, dan gebruik je best 7-zip. Hieronder overlopen we eerst enkele voorbeelden van software met ingebouwde encryptie. Daarna komt encryptie met 7-zip aan bod.

Encryptie met Microsoft Office

Om bijvoorbeeld met Microsoft Excel bestanden te versleutelen ga je naar het menu “Bestand”. Daar selecteer je “Werkmap Beveiligen” en vervolgens “Versleutelen met wachtwoord”.



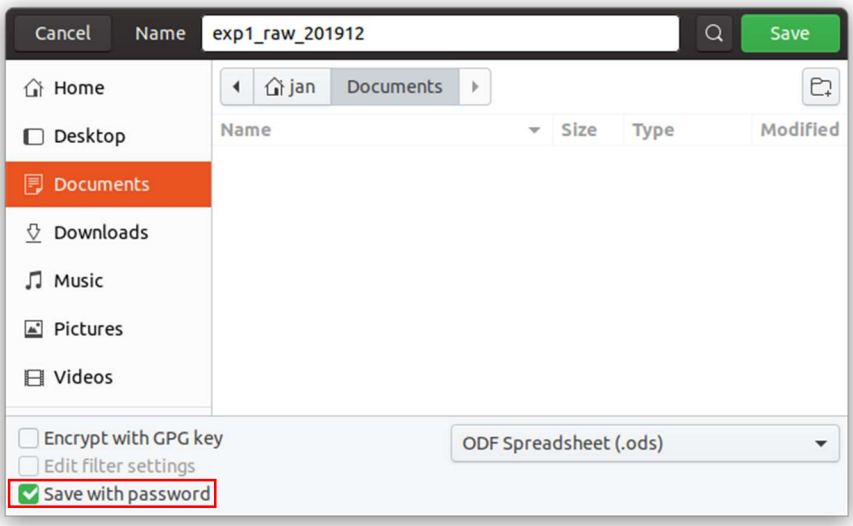
Vervolgens geef je een wachtwoord in.



Eens het wachtwoord is ingegeven moet je het document wel nog opslaan. Vanaf dat moment is je bestand beveiligd. Als je het document de volgende keer opent zal naar het wachtwoord gevraagd worden.

Encryptie met LibreOffice

Om bijvoorbeeld met LibreOffice Calc bestanden te versleutelen sla je het bestand op. In het opslagvenster selecteer je “Save with password”.

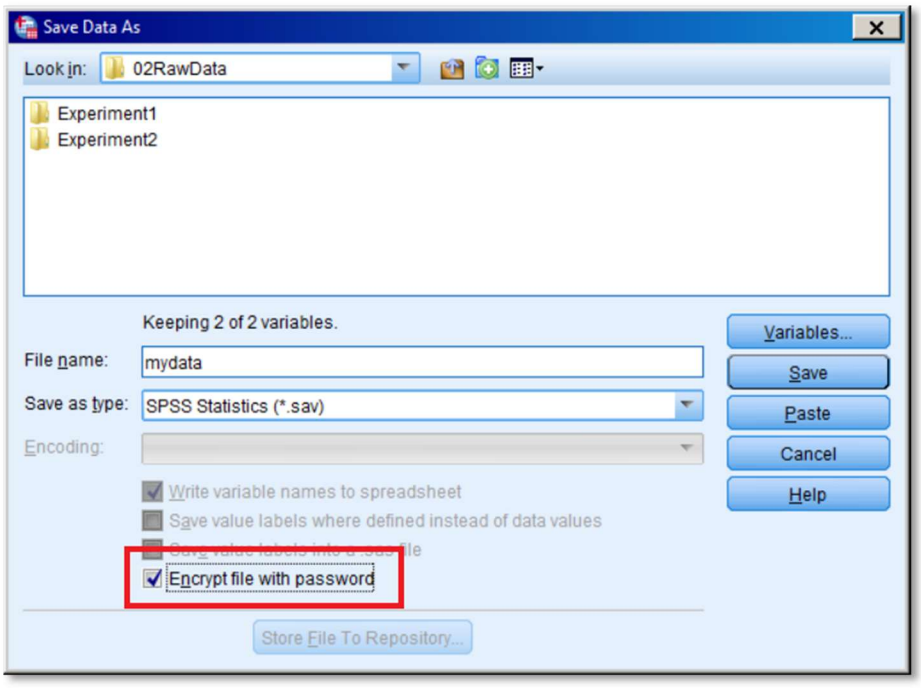


Vervolgens geef je een wachtwoord in.

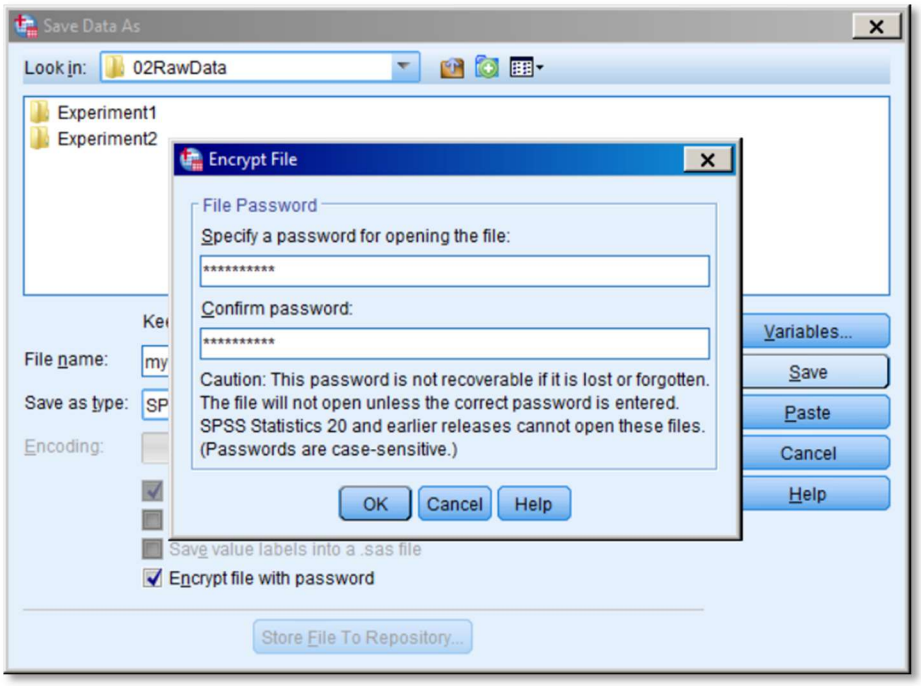
Eens het wachtwoord is ingegeven wordt het bestand versleuteld opgeslagen. Als je het document de volgende keer opent zal naar het wachtwoord gevraagd worden.

Encryptie met SPSS

Om SPSS-bestanden te versleutelen sla je het bestand op. In het opslagvenster selecteer je "Encrypt file with password".



Vervolgens geef je een wachtwoord in.



Eens het wachtwoord is ingegeven wordt het bestand versleuteld opgeslagen. Als je het document de volgende keer opent zal naar het wachtwoord gevraagd worden.

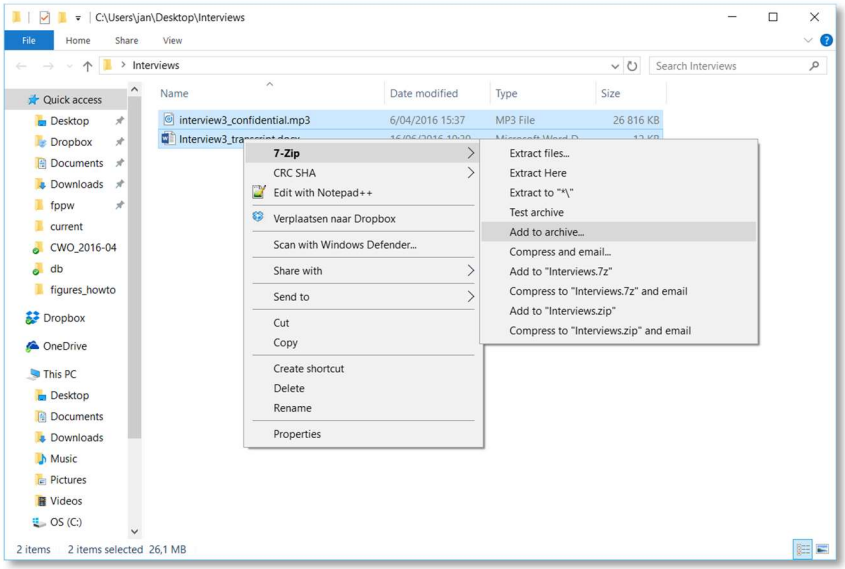
Encryptie met 7-zip

Op binnen de UGent uitgerolde computers wordt 7-zip standaard geïnstalleerd. Als 7-zip nog niet op je computer staat, ga dan naar http://www.7-zip.org, waar je de installatiebestanden kan downloaden. In dit voorbeeld gebruiken we de versie voor Windows.

Stel je hebt enkele bestanden die je in een versleuteld zip-bestand wil steken.

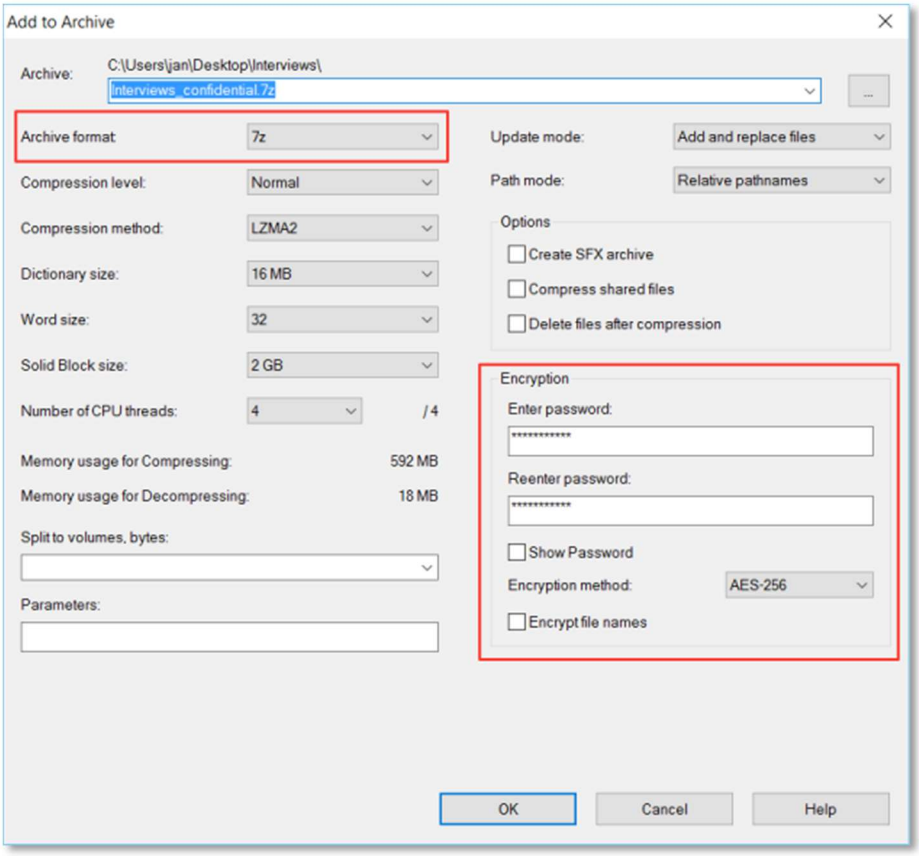
Stap 1

Ga naar de map waar deze bestanden zich bevinden. Selecteer de bestanden en druk op de rechtermuisknop. Als de installatie van 7-zip goed is verlopen, selecteer je “7-Zip” in het contextmenu en vervolgens “Toevoegen aan archief…”.



Stap 2

Je krijgt het volgende venster te zien



Zorg ervoor dat het “Archive format” op 7z staat en laat de “Encryption method” op AES-256 staan. Nadat je een passende naam hebt gegeven aan het zip-bestand, kan je een wachtwoord ingeven. Indien je de namen van de bestanden

in het zip-bestand ook onleesbaar wenst te maken, selecteer je “Encrypt file names”. Dit laatste is enkel aan te raden als de bestandsnamen op zichzelf ook vertrouwelijke informatie bevatten. Druk op “OK” en het versleutelde bestand wordt aangemaakt.

Als je dit zip-bestand deelt met anderen zullen zij ook 7-zip moeten installeren om de bestanden eruit te kunnen halen.

Hoe je versleutelde 7-zip-bestanden aanmaakt op MacOS en Linux vind je op http://www.howtogeek.com/203590/how-to-create-secure-encrypted-zip-or-7z-archives-on-any-operating-system/.

Scenario 3 – Projectfolder encrypteren

In dit dynamische scenario willen we een veilige plek maken waarin we gemakkelijk bestanden kunnen toevoegen en bewerken. Dit doen we aan de hand van een “encrypted file container”. Deze container kan gemakkelijk gedeeld worden, bv. via de cloud[3].

Folders encrypteren kan op verschillende manieren en met verschillende softwarepakketten. Eerst overlopen we hoe je hiervoor cryptomator kan gebruiken . Daarna gaan we dieper in op het gebruik van VeraCrypt.

Cryptomator

In dit voorbeeld gebruiken we de Windows versie van Cryptomator. Je vindt het installatiebestand van deze versleutelsoftware op https://cryptomator.org onder “Download”.

In Cryptomator wordt de “encrypted file container” een vault genoemd. Deze vault is eigenlijk een gewone folder die als beveiligde “kluis” dient om andere bestanden in op te bergen. Omdat het resultaat een folder is, betekent dit ook dat je er alles mee kan doen wat je met een gewone folder ook kan. Dit is heel flexibel: je kan de folder kopiëren, verplaatsen, hernoemen. Het houdt echter wel gevaren in waar je best rekening mee houdt: je kan de folder bijvoorbeeld gemakkelijk verwijderen.

We zullen eerst overlopen hoe je een nieuwe vault aanmaakt. Daarna gaan we dieper in op het dagelijkse gebruik. Samengevat gebruik je cryptomator als volgt:

Voorbereiding (Slechts eenmaal):

1. Cryptomator opstarten
2. Locatie en naam voor vault kiezen
3. Wachtwoord instellen

Bij elk gebruik:

1. Cryptomator opstarten
2. Vault selecteren en openen (Unlock)
3. Werken
4. Vault sluiten (Lock)

Een nieuwe vault maken

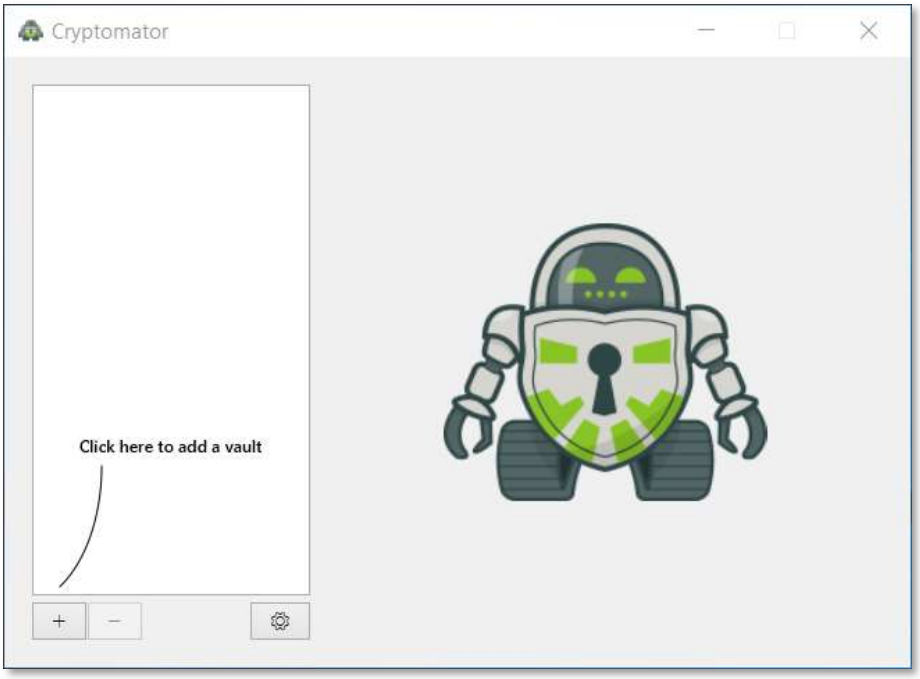
Het aanmaken van een vault is vrij eenvoudig. Het erop neer dat je moet kiezen waar je de vault wil plaatsen en hoe deze moet heten. Vervolgens kies je ook een wachtwoord.

We overlopen het proces stap voor stap:

[3] Zie ook punt 8 in Aandachtspunten voor veilig werken met IT-middelen

Stap 1 – Cryptomator starten

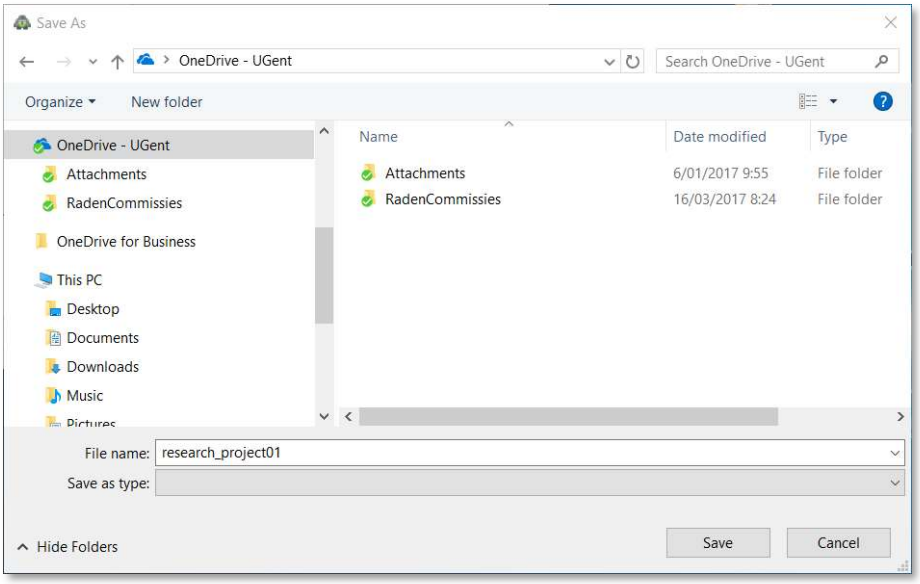
Eerst start je Cryptomator op. Je krijgt het volgende scherm te zien.



Om te beginnen druk je op "+" en selecteer je "create new vault" om een nieuwe vault aan te maken.

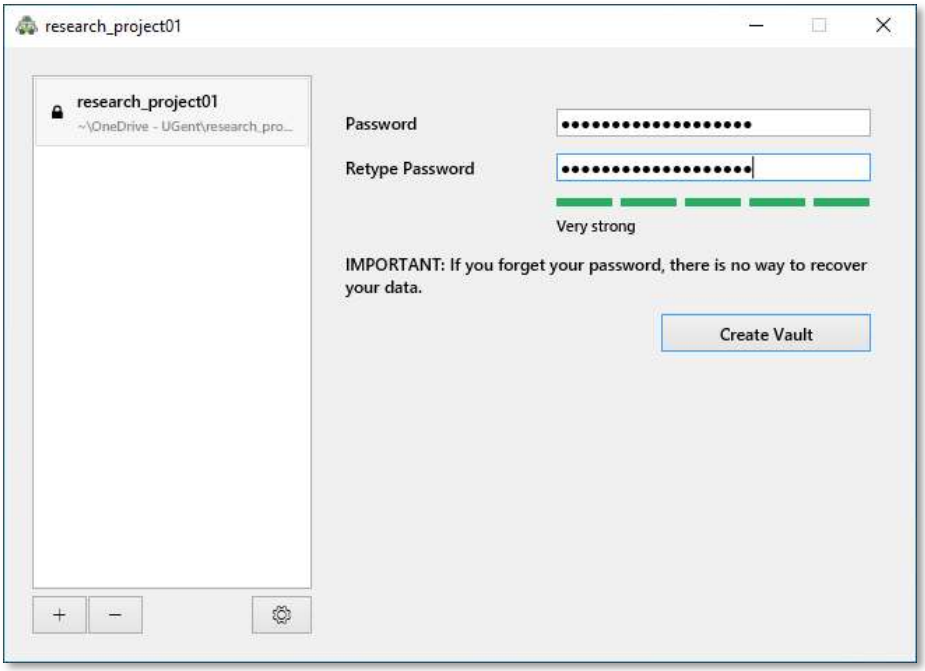
Stap 2 – Locatie en naam kiezen

In dit voorbeeld willen we een nieuwe vault aanmaken, dus selecteren we een locatie (hier de OneDrive for Business folder) en kiezen we een gepaste naam (in het voorbeeld "research_project01"). Eens je dit gedaan hebt druk je op save.



Stap 3 – Wachtwoord instellen

Eens de locatie en naam zijn gekozen verschijnt je vault links in het selectievenster. Nu kies je een sterk wachtwoord. Daarna druk je op "Create Vault" om de kluis aan te maken.



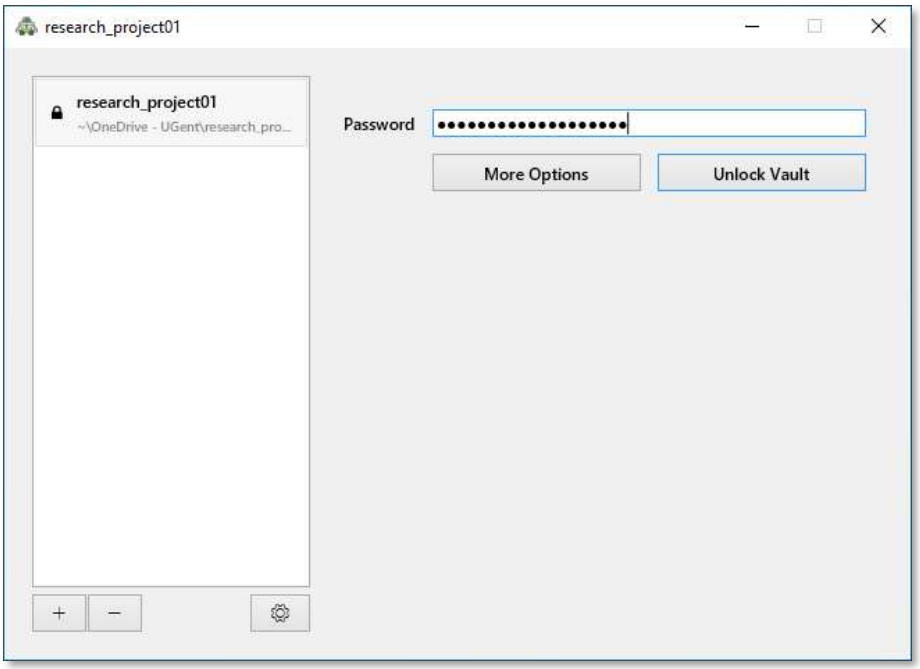
Een vault gebruiken op je PC

Het gebruik van een vault verloopt altijd via een vast patroon. Belangrijk is dat je steeds begint met het openen van je vault in cryptomator en dat je op het einde de kluis weer sluit. Hierover volgt later meer informatie.

Om de vault op een handige manier te kunnen gebruiken koppelt Cryptomator deze aan een virtuele schijf. Als de vault gekoppeld is lijkt het alsof je een extra schijf hebt op je computer. Je kan er net zo op werken als op een gewone schijf. Dit betekent ook dat zolang deze "virtuele" schijf aangekoppeld blijft, de inhoud ervan beschikbaar is voor iedereen die toegang heeft tot je computer. Als je klaar bent met het werken op de virtuele schijf dien je deze te ontkoppelen ("Lock vault"). Vergeet je dit, dan blijft de inhoud van de vault toegankelijk voor iedereen die toegang heeft tot je computer tot je je computer uitschakelt.

Stap 1 – Vault openen

Nadat je cryptomater hebt opgestart, is de eerste stap het openen van je vault. Dit doe je door de vault die je wil openen te selecteren. Vervolgens geef je het wachtwoord in en druk je op "Unlock vault".



Noot: Als je een vault wil openen die je nog nooit eerder hebt gebruikt op de computer waarmee je aan het werken bent, zal je deze vault niet zien staan in de lijst met beschikbare vaults (het linkerdeel van het venster). Dit kan bijvoorbeeld als je een vault hebt aangemaakt met je desktop PC op OneDrive en je deze bijvoorbeeld wil openen op je laptop.

Om een bestaande vault toe te voegen aan de selectielijst in cryptomator druk je op + en selecteer je "Open existing vault". Vervolgens ga je op zoek naar de folder met de vault die je wil openen. In die folder staat een bestand met de extensie ".cryptomator". Als je dit bestand selecteert en opent zal de vault worden toegevoegd aan je lijst met beschikbare vaults.

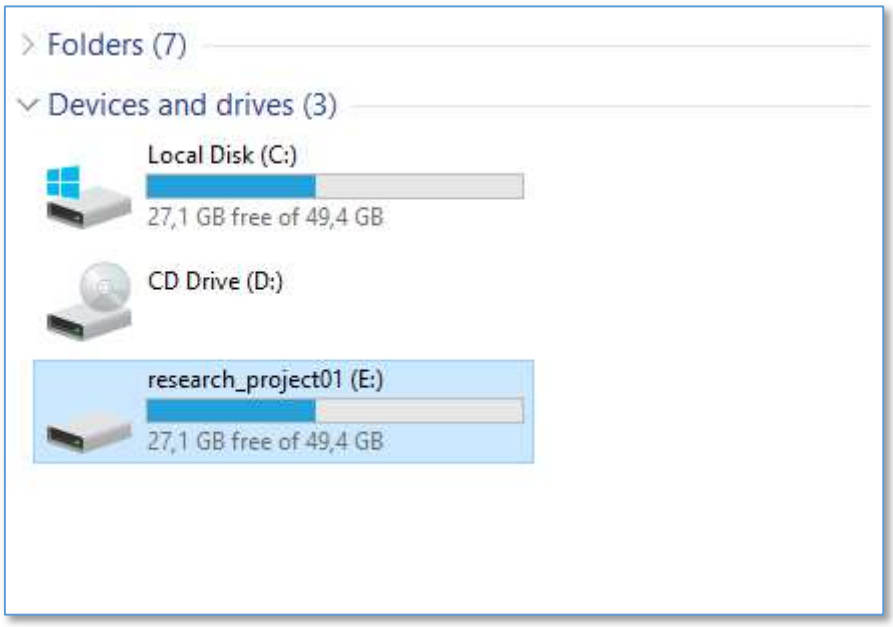
Eens dit is gedaan wordt de vault geopend en gekoppeld aan je systeem. Als je dit wil kan je nu het programmavenster van cryptomator minimaliseren.

In deze stap zijn er ook enkele opties die je terugvindt onder "more options". De belangrijkste zijn:

- *Drive Name*: Wil je dat de drive die aangemaakt wordt een andere naam krijgt dan de naam van je vault? Dan kan je dat hier instellen.
- *Save password*: wil je je wachtwoord niet telkens moeten ingeven? Dan kan je dit ook door cryptomator laten opslaan. Dit is af te raden.
- *Auto-Unlock on Start*: door deze optie wordt een de geselecteerde vault automatisch gekoppeld bij het opstarten van Windows. Dit is af te raden.
- *Custom Drive letter*: Wil je niet dat cryptomater zelf een drive-letter kiest om de virtuele schijf aan te koppelen? Dan kan je hier instellen welke drive-letter telkens moet gebruikt worden.

Stap 2 – Gebruiken

Je kan nu gewoon bestanden naar deze virtuele schijf schrijven via de Windows verkenner zoals je met een gewone schijf zou doen. Merk op dat de capaciteit van de virtuele schijf even groot is als de fysieke harde schijf waarop je ze gecreëerd hebt. In dit geval is dit de C:/-schijf omdat OneDrive daar een lokale kopie van zijn bestanden opslaat.



Stap 3 – Afkoppelen

Eens je klaar bent met de vorige stappen, moet je de vault nog sluiten. Dit doe je omdat personen die toegang hebben tot je computer natuurlijk ook toegang hebben tot de aangekoppelde vault.

Je gaat als volgt te werk: in Cryptomator selecteer je de schijf die je wil ontkoppelen en vervolgens druk je op “Lock vault”. Daarna wordt de virtuele schijf ontkoppeld en verdwijnt deze van je systeem. De inhoud van de vault is nu niet toegankelijk en wat overblijft is een folder met (onleesbare) gecodeerde bestanden.

VeraCrypt

Eerst overlopen we hoe je een “encrypted file container” aanmaakt met VeraCrypt. Daarna gaan we dieper in op het dagelijkse gebruik van zo’n container.

In dit voorbeeld gebruiken we de Windows versie van VeraCrypt. Je vindt het installatiebestand van deze versleutelsoftware op https://www.veracrypt.fr.

Samengevat gebruik je VeraCrypt als volgt:

Voorbereiding (Slechts eenmaal):

1. VeraCrypt opstarten
2. Volume creëren (encrypted file container)
3. Wachtwoord instellen

Bij elk gebruik:

1. VeraCrypt opstarten
2. Versleutelde container selecteren en koppelen (“mounten”) aan drive-letter.

3. Werken
4. Versleutelde container selecteren en ontkoppelen (“dismounten”).
5. VeraCrypt afsluiten

Een encrypted file container maken

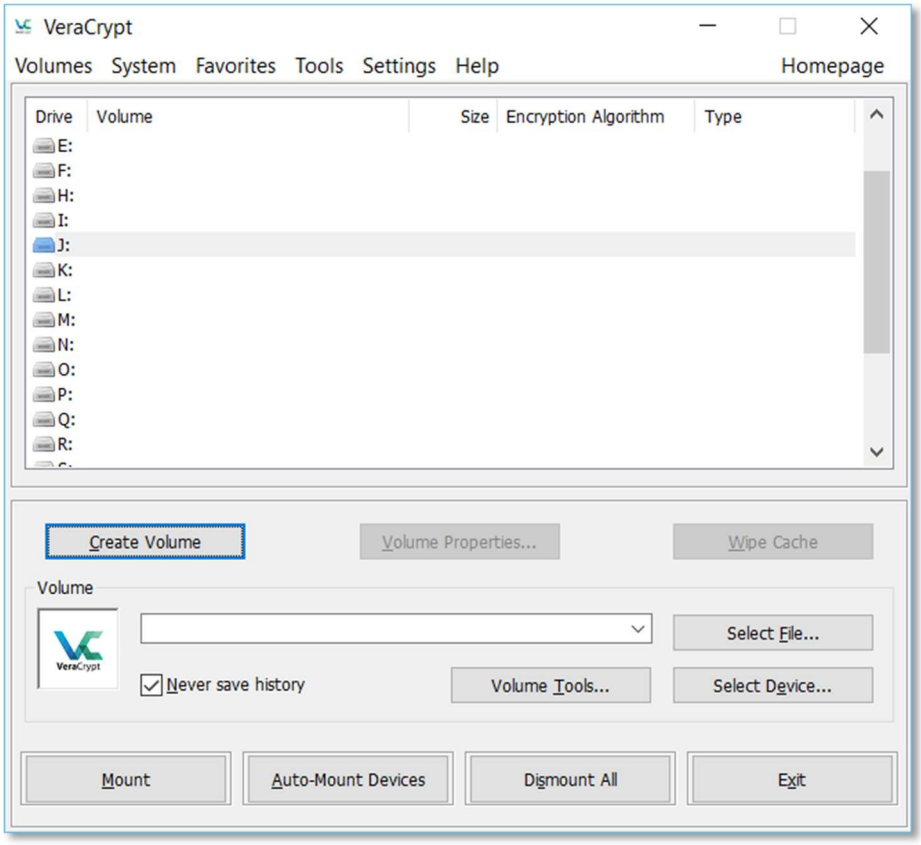
Een “encrypted file container” is een bestand dat als beveiligde “doos” dient om andere bestanden in op te bergen. Omdat het resultaat een bestand is, betekent dit ook dat je er alles mee kan doen wat je met een gewoon bestand ook kan. Dit is heel flexibel: je kan de container kopiëren, verplaatsen, hernoemen. Het houdt ook gevaren in waar je best rekening mee houdt: je kan de container gemakkelijk verwijderen.

Het aanmaken van een “encrypted file container” ziet er door het aantal te ondernemen stappen ingewikkeld uit, maar meestal worden de standaard instellingen gevolgd. Het komt erop neer dat je moet kiezen waar je de “encrypted file container” wil plaatsen, hoe deze moet heten en hoe groot hij moet zijn. Vervolgens kies je ook een wachtwoord.

We overlopen het proces nu stap voor stap:

Stap 1

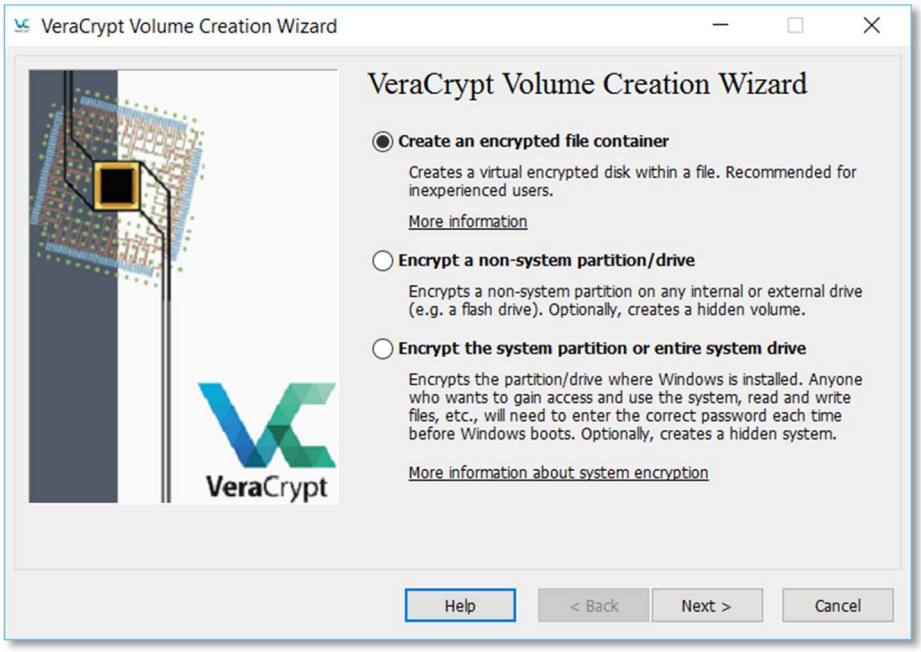
Eerst start je VeraCrypt op. Je krijgt het volgende scherm te zien.



Om te beginnen druk je op “Create Volume”.

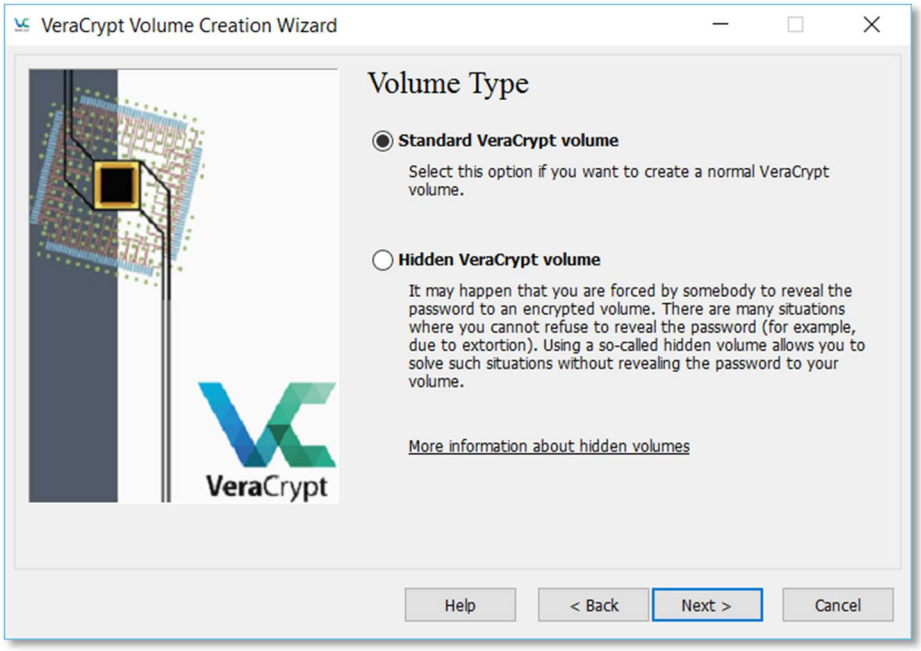
Stap 2

Standaard staat de optie voor een encrypted file container aangevinkt. Dit is wat we willen, dus klik “Next”.



Stap 3

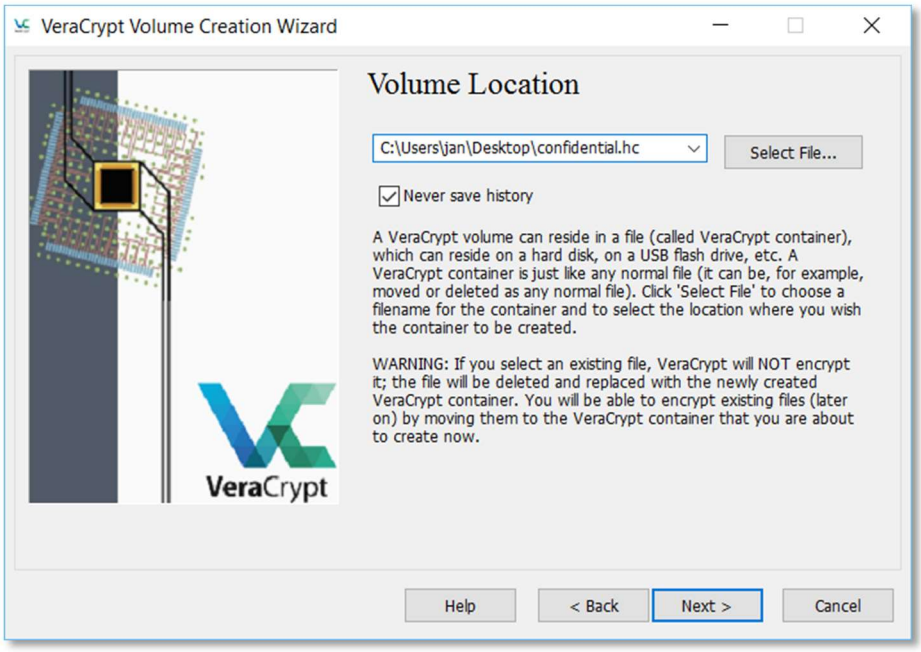
In deze stap wordt gevraagd welk type container je wil maken. Opnieuw kiezen we voor de standaard optie. Klik “Next”.



Stap 4

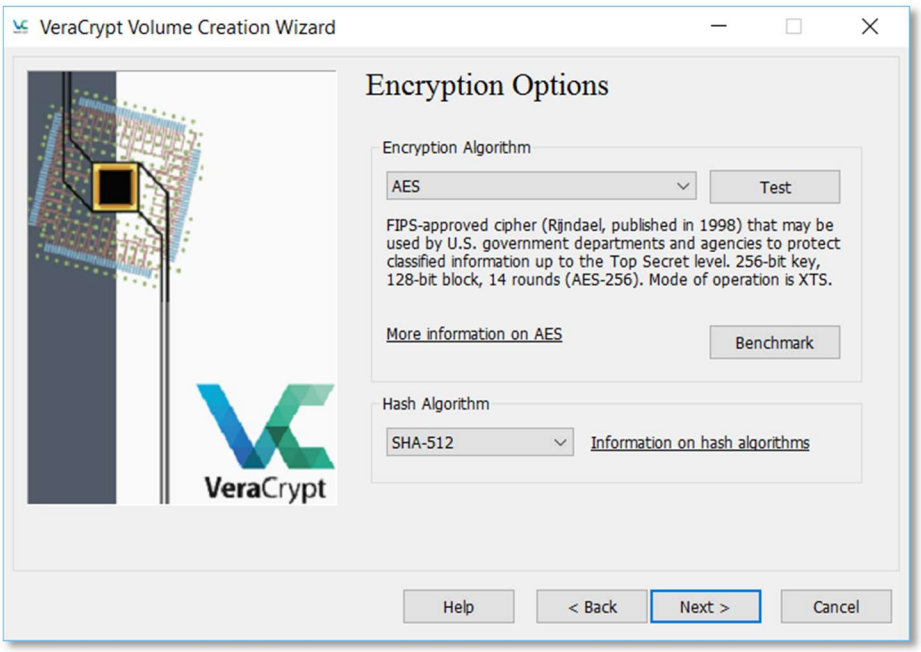
In de volgende stap dien je een locatie te zoeken voor de container die je wil maken. Klik op “Select file” en navigeer naar de plaats waar je het containerbestand wil plaatsen en geef het een naam. In het voorbeeld zal een bestand met de naam “confidential.hc” op het bureaublad worden gemaakt. Vaak wordt de extensie .hc gebruikt voor dit type bestanden, maar dit is niet verplicht (je mag de extensie dus ook achterwege laten). Indien je later het bestand op een andere

locatie wil plaatsen, dan is dit geen enkel probleem. Je kan het gewoon verplaatsen of kopiëren zoals een gewoon bestand.



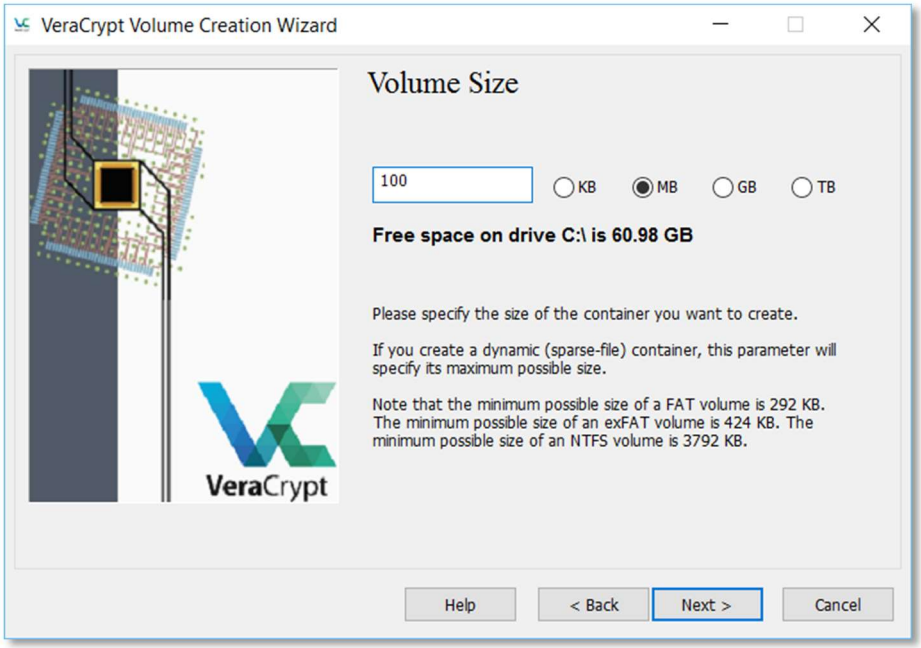
Stap 5

In de volgende stap worden de opties voor encryptie ingesteld. Tenzij je een expert bent en goede redenen hebt om van de standaardinstellingen af te wijken laat je deze gewoon staan. Klik op Next.



Stap 6

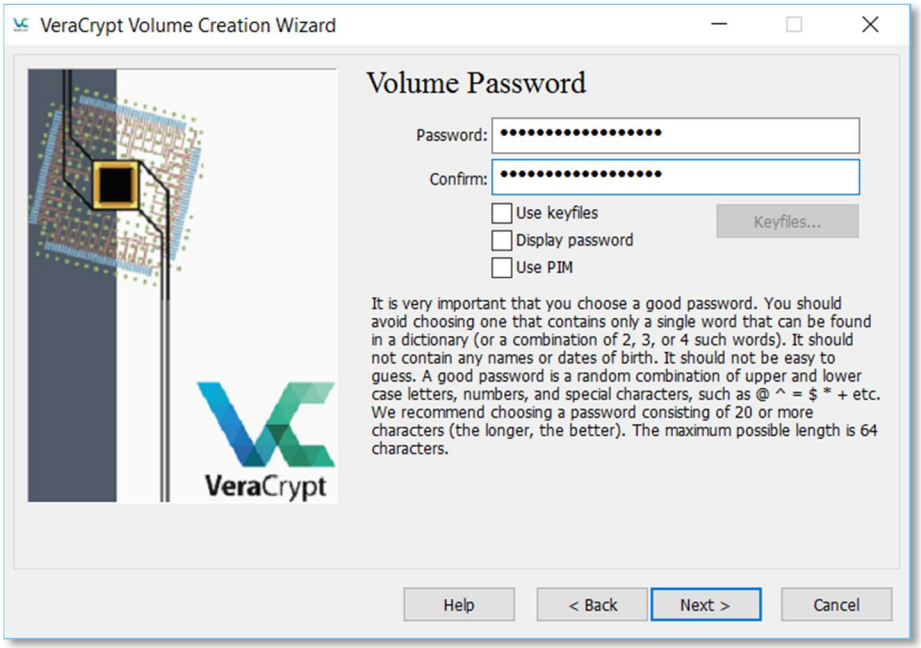
Bij de volgende stap kies je de grootte van het containerbestand. Het is belangrijk dat je hier goed over nadenkt. Kies de grootte niet overdreven groot als dit niet nodig is. Hoe groter het bestand hoe langer het zal duren om het bestand te versleutelen.



Stap 7

In stap 7 stel je het wachtwoord in.

Noot: Naast een traditioneel wachtwoord kan je voor extra beveiliging ook nog zogenaamde “keyfiles” gebruiken. Dit zijn unieke bestanden waarover je moet beschikken om de container te kunnen openen. Je kan het beschouwen als extra sleutels op het slot. Deze keyfiles kunnen met VeraCrypt gemaakt worden, maar je kan ook eigen bestanden gebruiken (bv. een foto van je kat). Iedereen die de container wil openen moet dan deze bestanden hebben én het wachtwoord

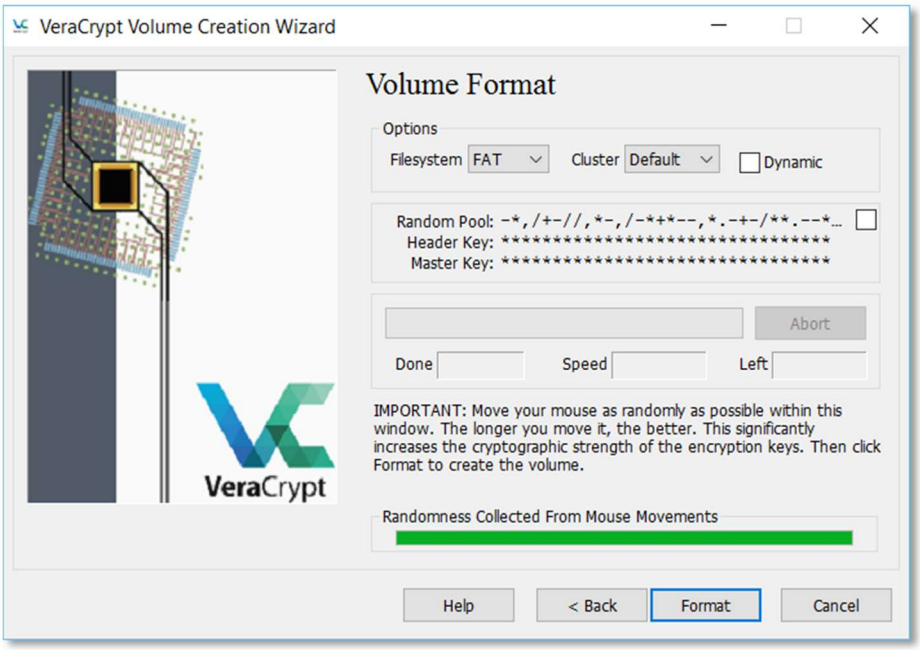


weten. In dit voorbeeld beperken we ons tot versleuteling met een gewoon wachtwoord, zonder gebruik te maken van keyfiles.

Stap 8

In de laatste stap wordt gevraagd om de encryptie te versterken door “randomness” of willekeur toe te voegen aan het versleutelingsalgoritme. Dit doe je door op een willekeurige manier met je muiscursor over het scherm te bewegen tot het balkje onderdaan volledig groen is.

Eens dit is gebeurd kan je je container finaliseren door op “Format” te klikken.



Dit kan even duren, zeker als je een grote container wil maken. Na het formatteren van je container, vind je het bestand terug op de locatie die je in Stap 4 opgaf.

Noot: de optie “Filesystem” staat in deze stap standaard ingesteld op “FAT”. Dit is meestal voldoende en alle besturingssystemen kunnen hiermee overweg. In sommige situaties kan het echter beter zijn om “exFAT” te gebruiken. Bv. als je van plan bent om grote bestanden (>4GB) naar je “encrypted file container” te schrijven.

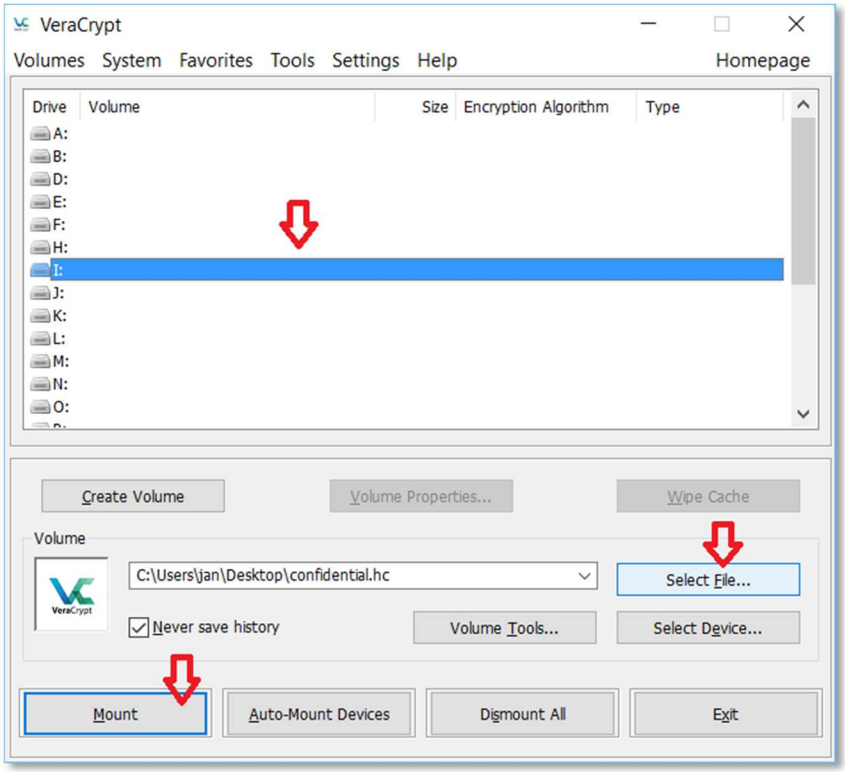
Een encrypted file container gebruiken

Het gebruik van een encrypted file container verloopt altijd via een vast patroon: VeraCrypt openen, container koppelen, werken, container ontkoppelen.

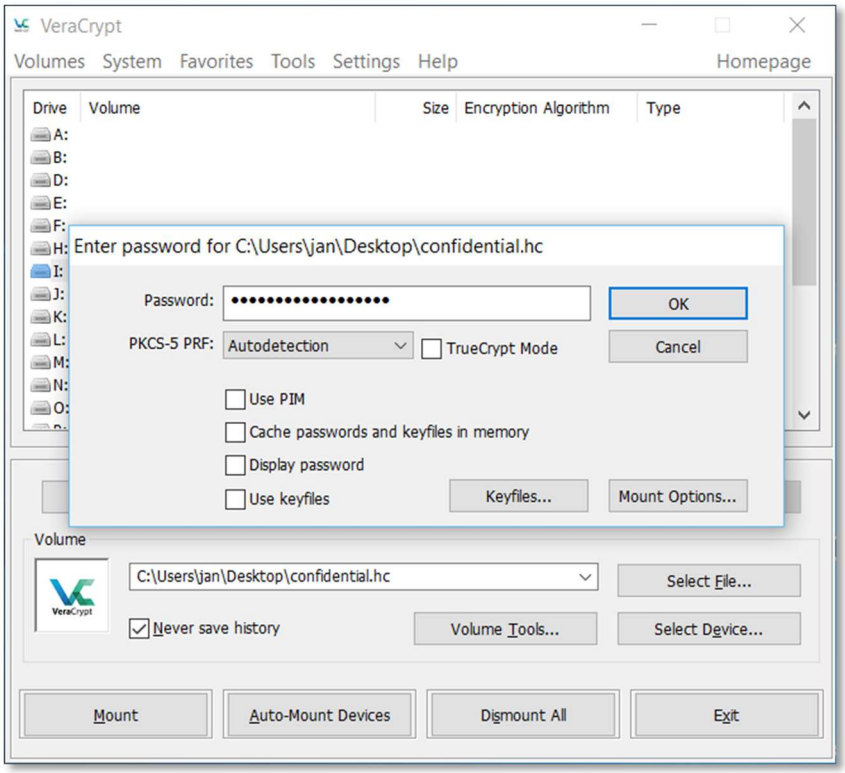
Om de container op een handige manier te gebruiken koppelt VeraCrypt het aangemaakte bestand aan een virtuele schijf (“Mounten”). Als de container is gekoppeld lijkt het alsof je een extra harde schijf hebt op je computer. Je kan er net zo op werken als op een gewone harde schijf. Dit betekent ook dat zolang deze “virtuele” schijf aangekoppeld blijft de inhoud ervan beschikbaar is voor iedereen die toegang heeft tot je computer. Als je klaar bent met het werken op de virtuele schijf moet je deze ontkoppelen (“Dismounten”). Bij het ontkoppelen wordt de inhoud versleuteld. Ben je vergeten te ontkoppelen voordat je je computer uitzet? In principe is dit geen probleem omdat de container automatisch wordt ontkoppeld en versleuteld wanneer je je computer uitzet.

Stap 1 – Aankoppelen

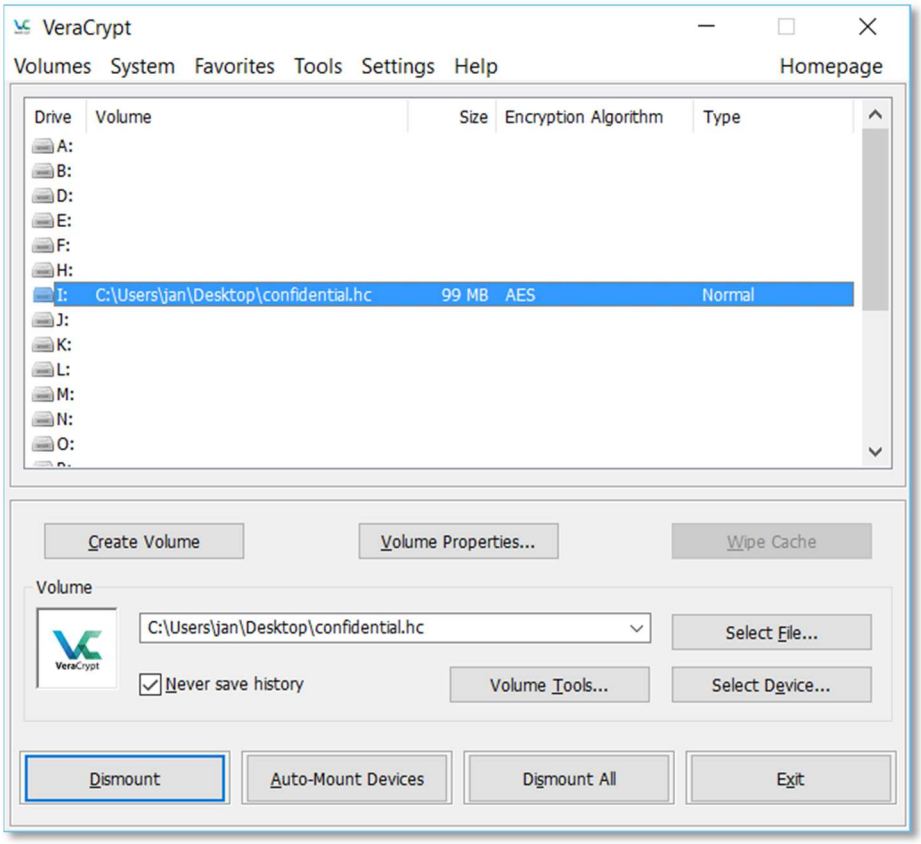
De eerste stap is het aankoppelen van je encrypted file container aan een harde schijf. In Windows betekent dit dat je een schijfletter selecteert waarop je wil aankoppelen alsook de container die je wil aankoppelen. Vervolgens klik je op "Mount".



Er wordt je vervolgens gevraagd om het wachtwoord in te geven.



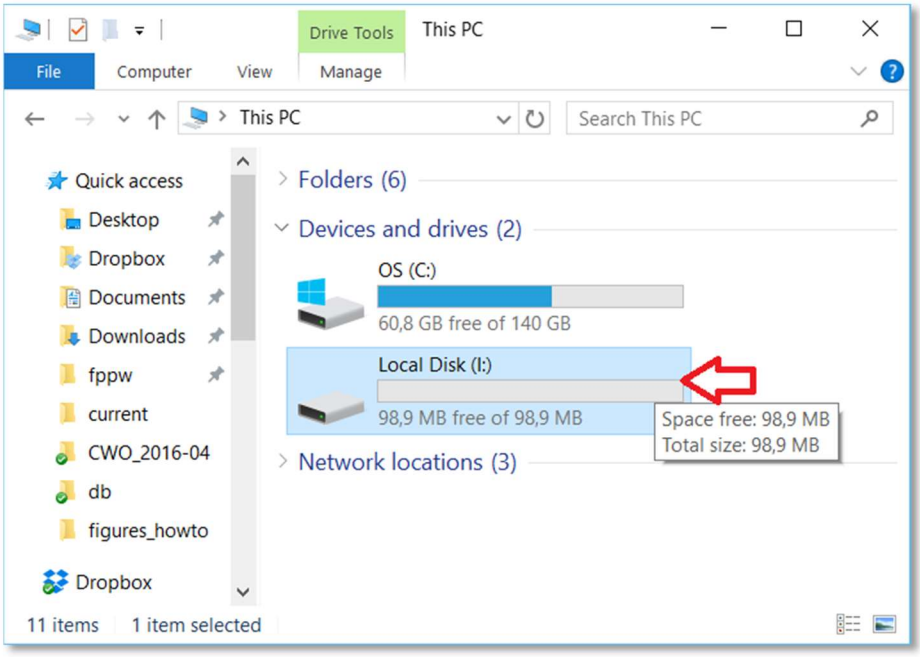
Eens dit is gedaan wordt de encrypted file container ontsloten en gekoppeld aan je systeem. Het gevolg is dat er een nieuwe lokale schijf bij komt op je computer (in dit geval onder de schijfletter I:\).



Als je dit wil kan je nu het venster van VeraCrypt verkleinen of sluiten.

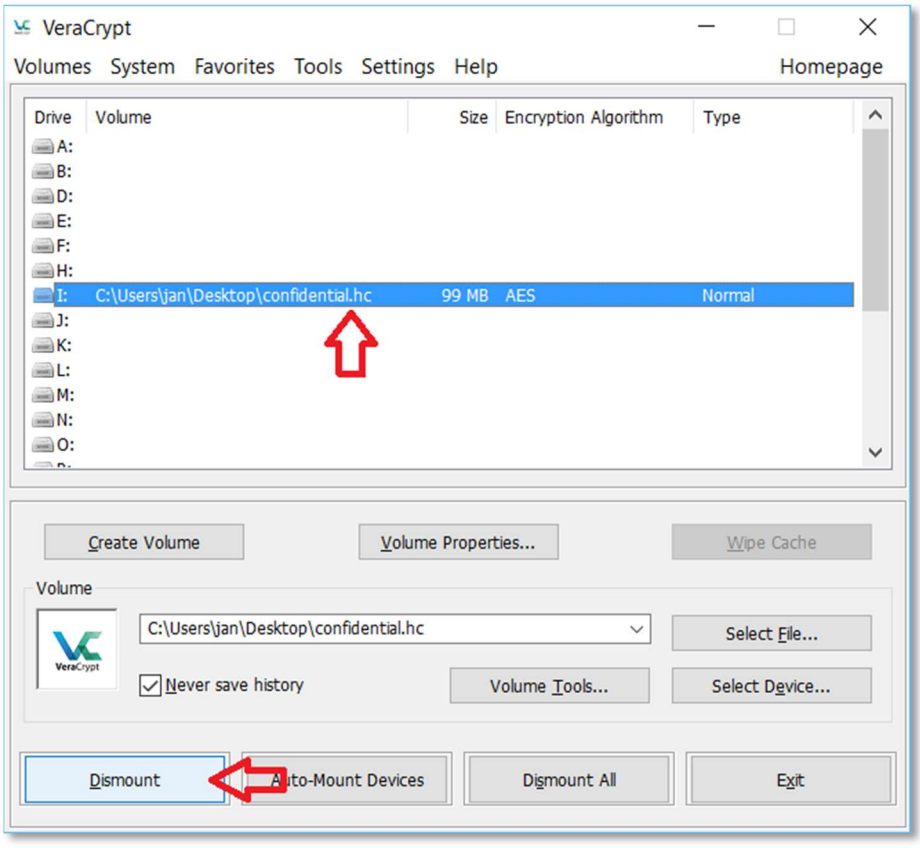
Stap 2 – Gebruiken

Je kan nu gewoon bestanden naar deze lokale schijf schrijven via de Windows verkenner zoals je met een gewone schijf zou doen.



Stap 3 – Afkoppelen

Eens je klaar bent met je werk dien je de file container nog te ontkoppelen. Als je dit niet manueel doet wordt de file container automatisch ontkoppeld wanneer je je computer uitzet. Wees je ervan bewust dat zolang je dit niet hebt



gedaan, mensen die toegang hebben tot je computer ook toegang hebben tot de (vertrouwelijke) bestanden in de file container.

Je gaat als volgt te werk: eerst selecteer je in Veracrypt de schijf die je wil ontkoppelen en vervolgens druk je op “Dismount”. Vervolgens wordt de virtuele schijf afgekoppeld en verdwijnt deze van je systeem. De file container is nu versleuteld en wat overblijft is het (onleesbare) gecodeerde bestand waar je in stap 1 mee begon.

Scenario 4 – Externe devices encrypteren

In dit voorbeeld overlopen we hoe je een externe harde schijf of usb-stick kan versleutelen. Dit komt grotendeels overeen met het aanmaken van een encrypted file container (zie “Scenario 3 – Projectfolder encrypteren met VeraCrypt”), maar in plaats van gebruik te maken van een versleuteld bestand, wordt nu gebruik gemaakt van een fysieke schijf of USB-stick.

Het gebruik van VeraCrypt in dit scenario is vooral van toepassing wanneer het versleutelde medium gebruikt zal worden op verschillende besturingssystemen. Stel: jij werkt met MacOS en je collega met Windows. Indien je dan een versleutelde usb-stick wil maken die door beiden moet kunnen worden gelezen, gebruik je best VeraCrypt. Indien je het medium niet binnen verschillende besturingssystemen moet kunnen gebruiken, dan is het handiger om versleutelsoftware van je besturingssysteem te gebruiken (Bitlocker voor Windows, FileVault2 voor MacOS).

Samengevat gebruik je VeraCrypt als volgt:

Voorbereiding (Slechts eenmaal):

1. VeraCrypt opstarten
2. Encrypted Volume creëren
3. Wachtwoord instellen

Bij elk gebruik:

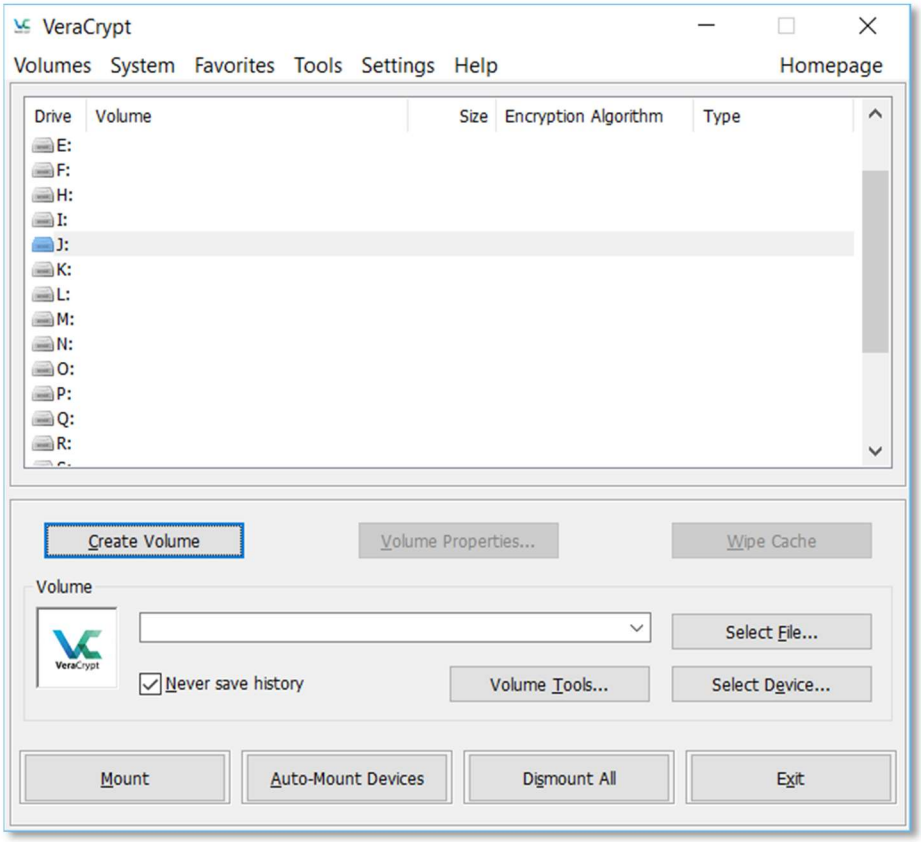
5. VeraCrypt opstarten
6. Versleuteld device selecteren en drive-letter kiezen en “Mounten”.
7. Werken
8. Versleuteld device selecteren in VeraCrypt en “Dismounten”.
9. VeraCrypt afsluiten

Een versleutelde schijf voorbereiden

Vooraleer je een versleutelde schijf of usb-stick kan gebruiken moet je deze eerst voorbereiden. Hiervoor doorloop je onderstaande stappen. Dit hoef je maar eenmaal te doen.

Stap 1

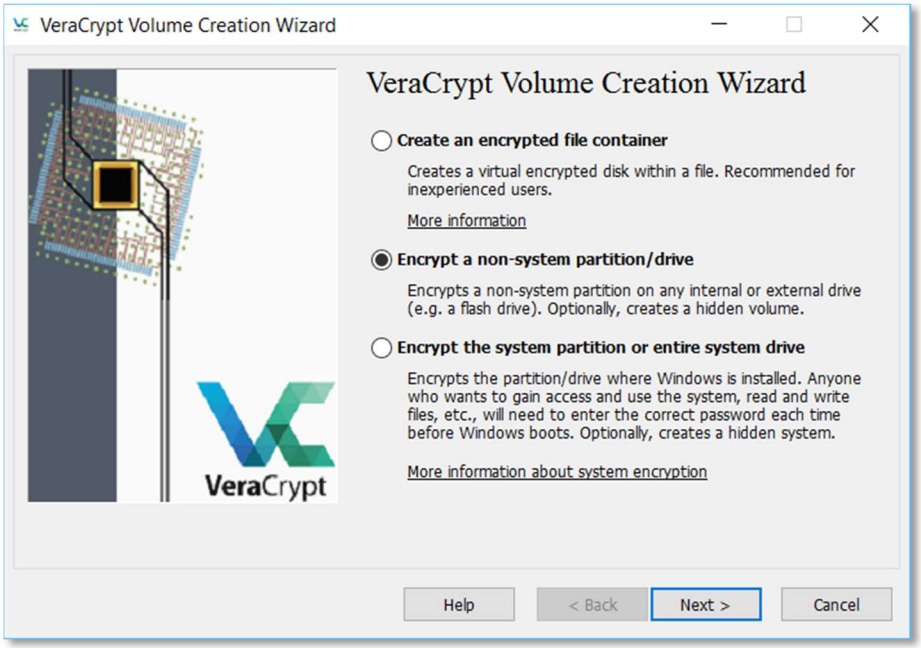
Eerst start je VeraCrypt op. Je krijgt het volgende scherm te zien.



Om te beginnen druk je op “Create Volume”.

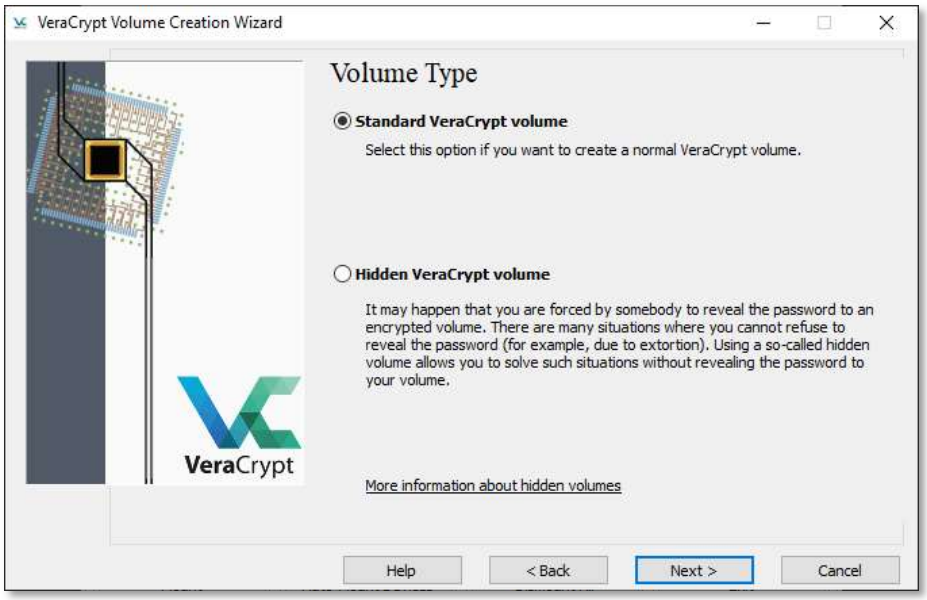
Stap 2

Standaard staat de optie voor een encrypted file container aangevinkt. Dit is NIET wat we hier willen. We willen namelijk een schijf encrypteren die niet de systeemschijf is (Bv. een externe usb-schijf of een usb-stick). Om dit te doen selecteren we de tweede optie “Encrypt a non-system partition/drive” en dan “Next”.



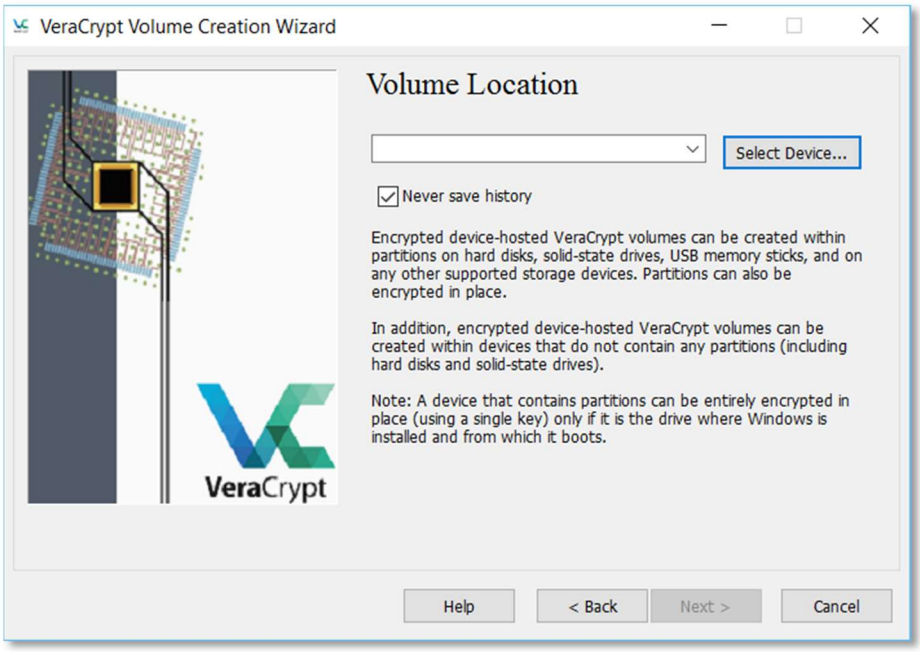
Stap 3

Vervolgens word je gevraagd of je een normaal VeraCypt volume wil maken, dan wel een verborgen volume. Deze tweede optie kan van pas komen in heel specifieke omstandigheden, maar meestal volstaat de standaard optie.

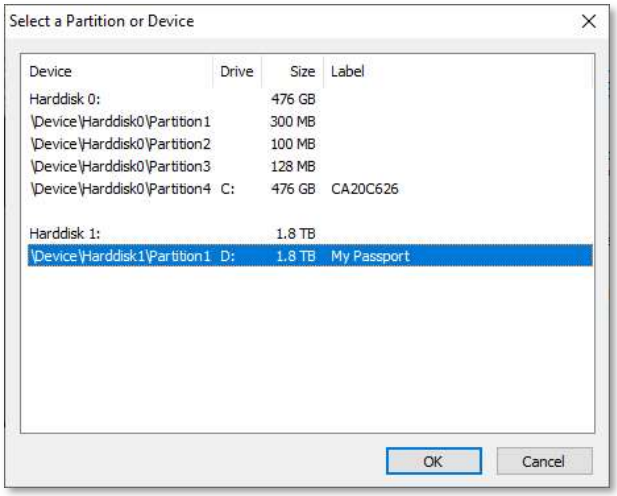


Stap 4

In de volgende stap dien je de locatie op te geven van de harde schijf die je wil encrypteren. Om dit te doen klik je op “Select device”.



Je krijgt het volgende venster te zien.

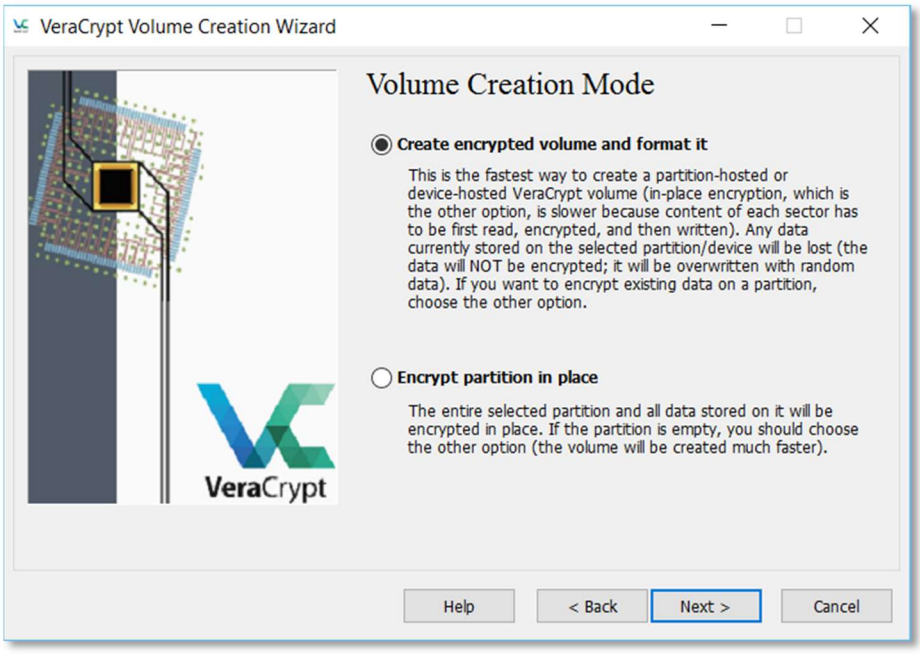


In dit voorbeeld is de verwijderbare harde schijf die we willen versleutelen aangekoppeld aan de schijfletter D:. We selecteren deze schijf en drukken op "OK".

Noot: Let op! Het is heel belangrijk dat je de juiste schijf selecteert. Als je weet hoe groot de externe harde schijf is, kan je dit vergelijken met de opgegeven grootte in de "Size" kolom. Hou er wel rekening mee dat de echte grootte van een schijf steeds iets kleiner is dan de aangegeven grootte op de verpakking van je schijf. In het voorbeeld gebruiken we een schijf van 2TB. Echter, in het lijstje staat dat deze slechts 1.8TB groot is. Weet je niet hoe groot je schijf is, open dan de Windows verkenner voor je de harde schijf aan je computer aansluit. Sluit vervolgens de harde schijf aan en kijk welke schijfletter erbij komt. Twijfel je nog altijd, vraag dan advies, bv. bij je ICT-verantwoordelijke.

Stap 5

In de volgende stap kies je wat er zal gebeuren met de data die (eventueel) reeds op de harde schijf staan. Is de schijf leeg, of staan er data op die je niet meer wenst te behouden, selecteer dan de eerste optie "Create encrypted volume and format it". Door deze optie te selecteren zullen alle data die op de schijf staan worden verwijderd vooraleer ze wordt versleuteld. Dit is de snelste optie.

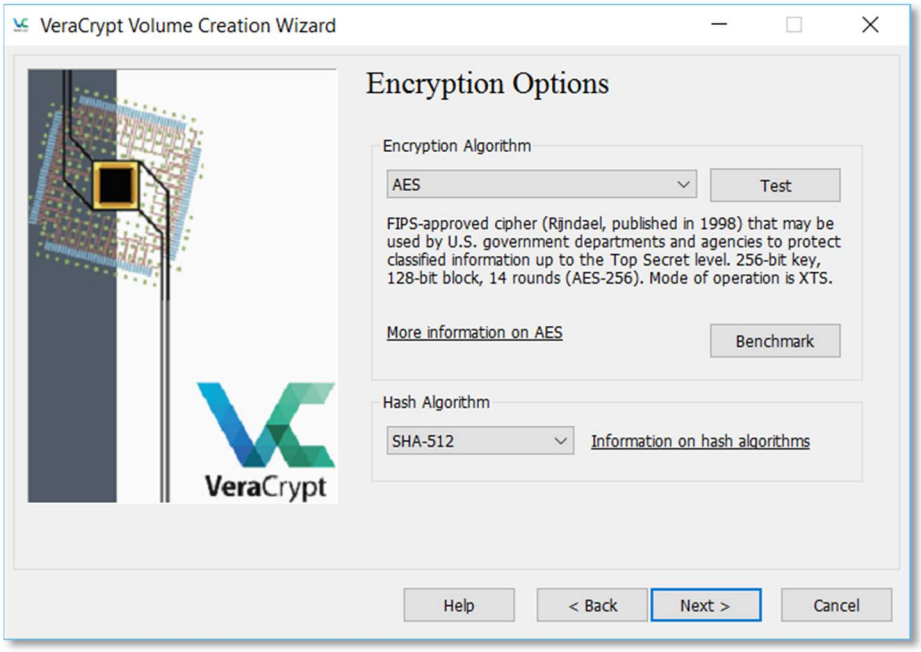


Indien je de data die reeds op de schijf staan wil bewaren en versleutelen dien je de tweede optie te selecteren ("Encrypt partition in place"). Omdat er niet van een lege schijf wordt vertrokken, zal het uitvoeren van deze optie meer tijd in beslag nemen.

Wanneer je je keuze hebt gemaakt druk je op "Next".

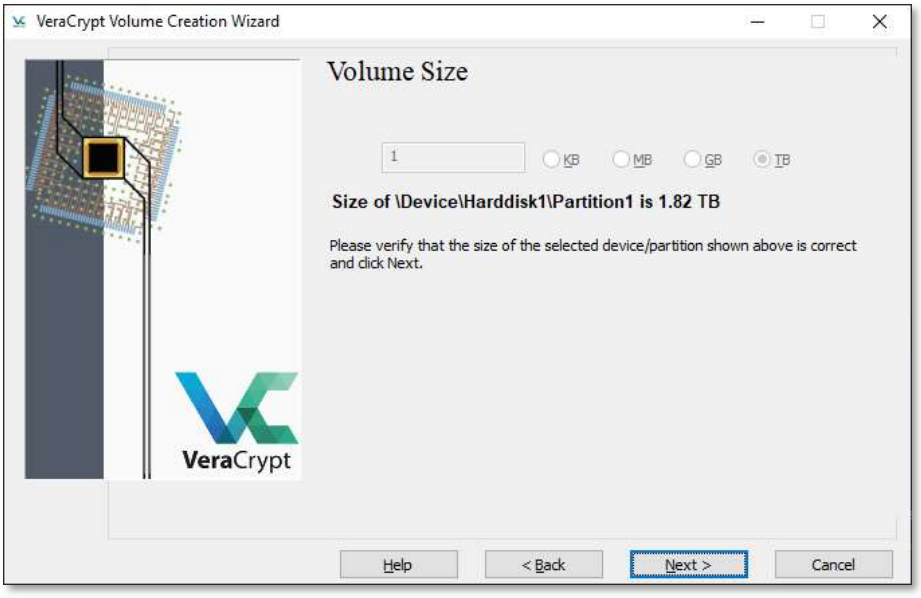
Stap 6

In de volgende stap worden de opties voor encryptie ingesteld. Tenzij je een expert bent en goede redenen hebt om van de standaard instellingen af te wijken laat je deze gewoon staan. Druk op "Next".



Stap 7

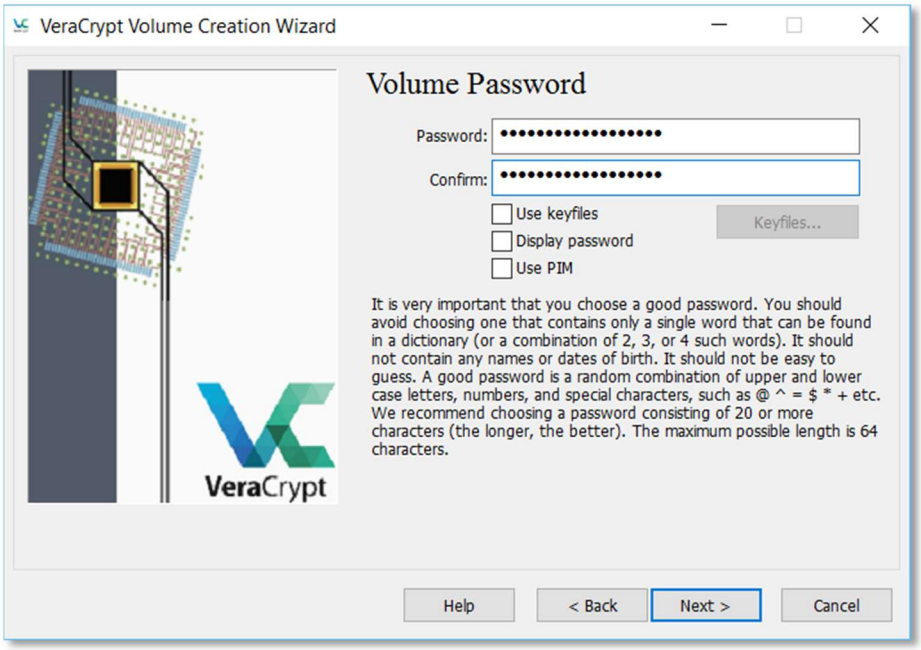
Bij de volgende stap wordt de grootte van het volume nog eens getoond. Omdat we de hele harde schijf aan het versleutelen zijn, is deze stap louter informatief en kan je niks wijzigen. Druk op "Next".



Stap 8

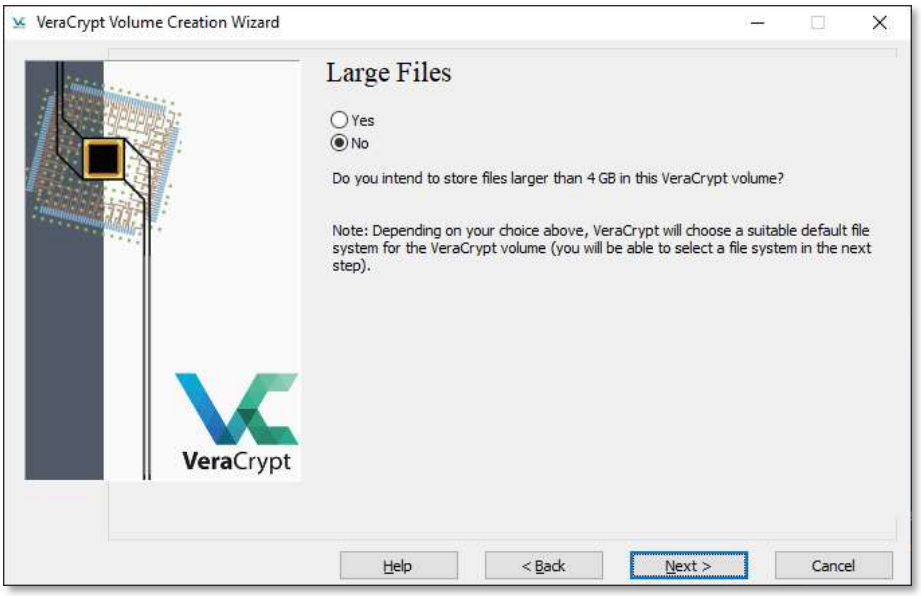
In stap 8 stel je het wachtwoord in.

Noot: Naast een traditioneel wachtwoord kunnen voor extra beveiliging ook nog zogenaamde keyfiles gebruikt worden. Dit zijn unieke bestanden waarover je moet beschikken om de container te kunnen openen. Je kan het beschouwen als extra sleutels op het slot. Deze keyfiles kunnen met VeraCrypt gemaakt worden, maar je kan ook eigen bestanden gebruiken (bv. foto van je kat). Iedereen die de container wil openen moet dan deze bestanden hebben én het wachtwoord weten. In dit voorbeeld beperken we ons tot versleuteling met een gewoon wachtwoord, zonder keyfiles te gebruiken.



Stap 9

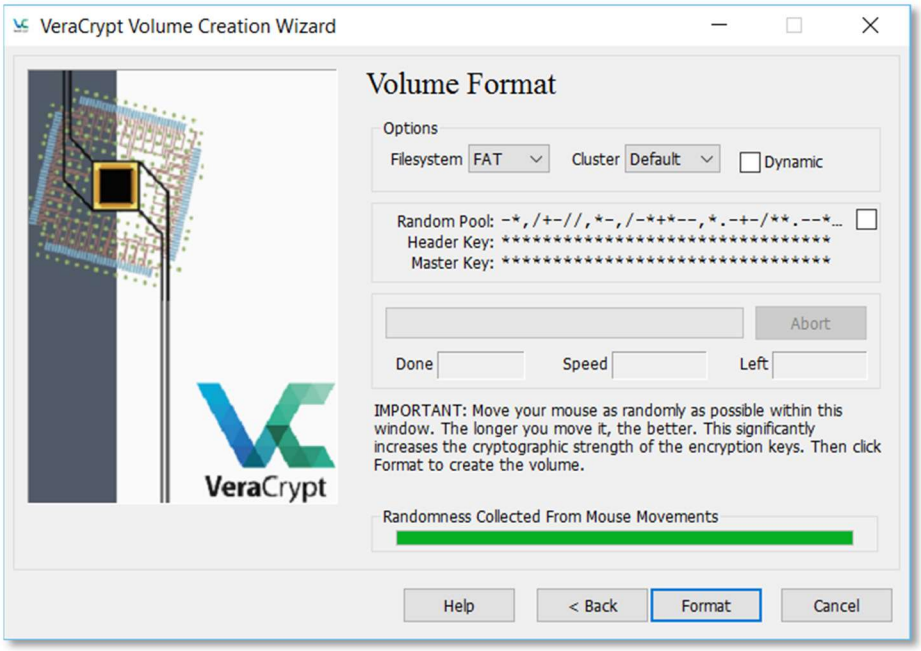
Indien je grote bestanden (>4GB) wil gebruiken op de versleutelde schijf, dan kan je dit in deze stap aangeven.



Stap 10

In de laatste stap wordt gevraagd om de encryptie te versterken door “randomness” of willekeur toe te voegen aan het versleutelingsproces. Dit doe je door op een willekeurige manier met je muiscursor over het scherm te bewegen tot het balkje onderdaan volledig groen is.

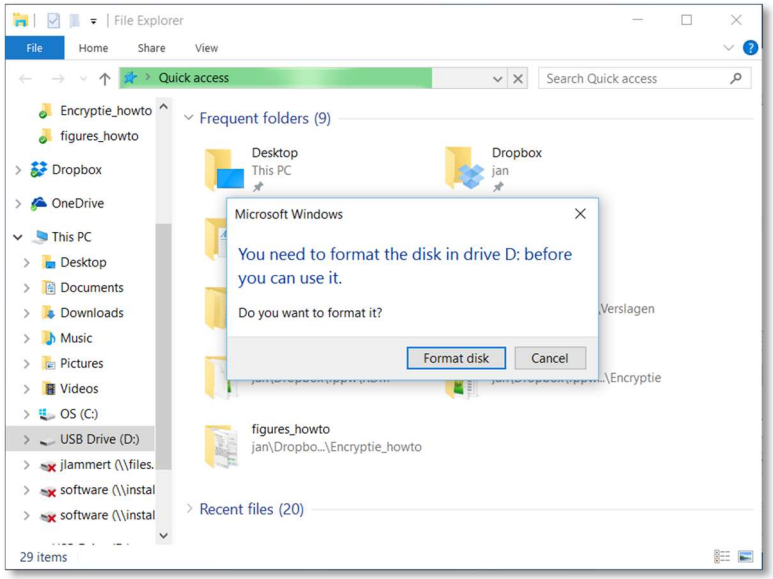
Eens dit is gebeurd kan je de encryptie van de schijf finaliseren door op “Format” te klikken.



Dit kan even duren, zeker als je een grote schijf wil versleutelen. Na het formatteren en versleutelen van je harde schijf vind je die nog niet terug op je systeem. Daarvoor moet je ze eerst aankoppelen.

De versleutelde harde schijf gebruiken

Opgelet! De inhoud van een versleutelde schijf is in principe onleesbaar voor een computer. Wanneer je de versleutelde schijf of usb-stick aansluit op je computer zal Windows je daarom vragen of je de schijf of usb-stick wil “formatteren”.



Doe dit zeker niet, want dan wordt de inhoud van de versleutelde schijf gewist! Klik dus in elk geval op “Cancel”. Om de versleutelde schijf aan te koppelen maken we opnieuw gebruik van VeraCrypt.

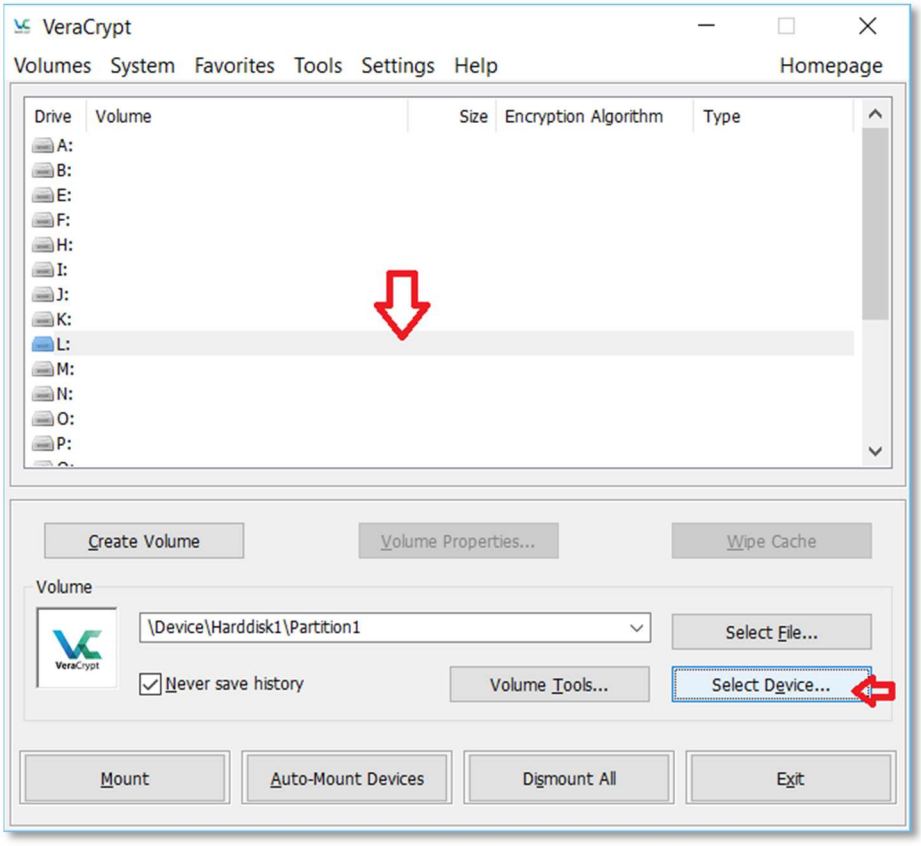
Het gebruik van een versleutelde harde schijf verloopt altijd via een vast patroon: VeraCrypt openen, device koppelen, werken, device afkoppelen.

Om de versleutelde schijf op een handige manier te kunnen gebruiken, koppelt VeraCrypt deze aan een virtuele schijf (“Mount”). Als de versleutelde schijf is gekoppeld lijkt het alsof je een extra harde schijf hebt. Je kan er net zo op werken als op een gewone harde schijf. Dit kan verwarrend zijn omdat de (onleesbare) harde schijf bij het aansluiten op je Windows-computer reeds een schijfletter kreeg toegewezen (in het voorbeeld is dit letter D:). Het activeren van de harde schijf met VeraCrypt zal er dus voor zorgen dat er nog een extra harde schijf zal bijkomen (letter L: in het voorbeeld, zie verder). Het is deze laatste die kan gebruikt worden om op te werken.

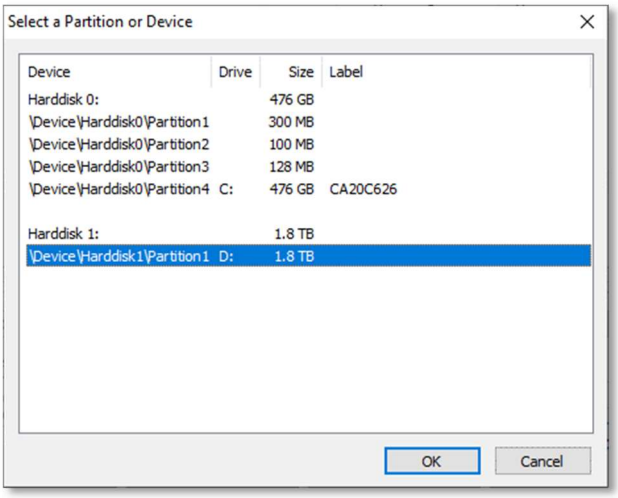
Zolang de “virtuele” schijf aangekoppeld is blijft de inhoud ervan beschikbaar voor iedereen die toegang heeft tot je computer. Daarom is het een goed idee om de virtuele schijf te ontkoppelen (“Dismount”) als je deze niet meer nodig hebt. Indien je de schijf niet manueel ontkoppelt, zal dit automatisch gebeuren wanneer je je computer uitzet.

Stap 1 – Aankoppelen

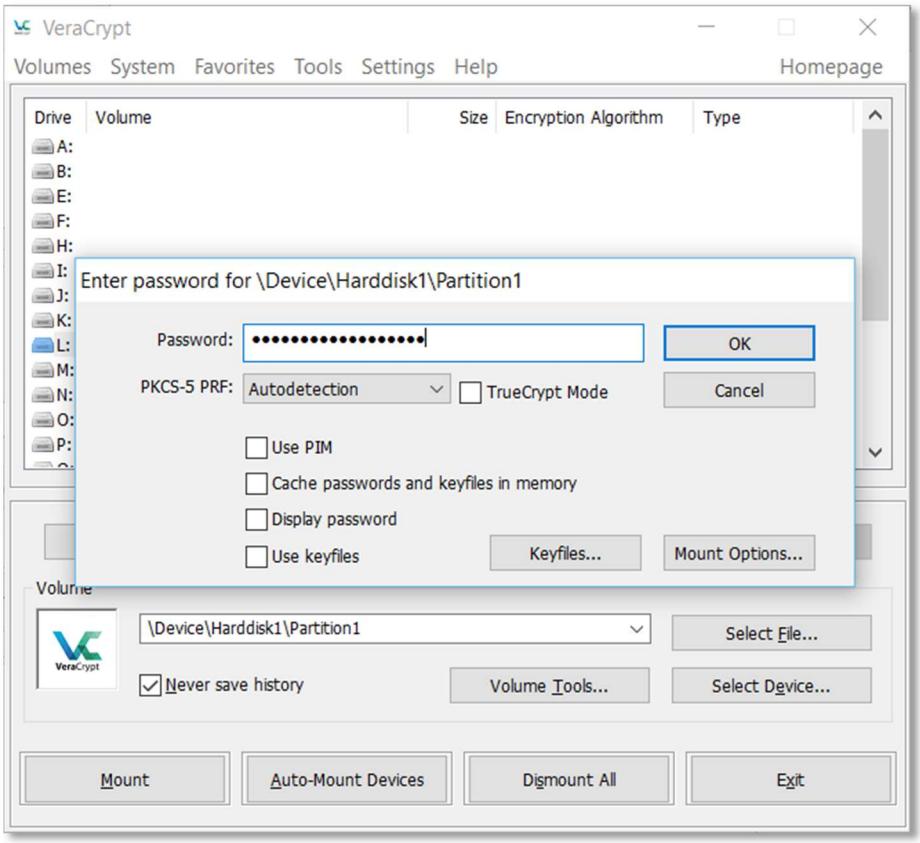
De eerste stap is het aankoppelen van je versleutelde harde schijf. In Windows betekent dit dat je een schijfletter selecteert waarop je wil aankoppelen alsook het “device” dat je wil aankoppelen.



In het een overzicht van de beschikbare schijfletters kies je eerst een schijfletter waarop je de versleutelde schijf wil op aankoppelen. Selecteer dan “Select device” om de versleutelde schijf te kiezen die je wil aankoppelen.



Selecteer de versleutelde schijf en druk “Ok”. Je hebt nu de je versleutelde schijf geselecteerd en de letter waarop je deze wil koppelen. Druk vervolgens op “Mount”. Omdat de schijf versleuteld is wordt je gevraagd om het wachtwoord in te geven.



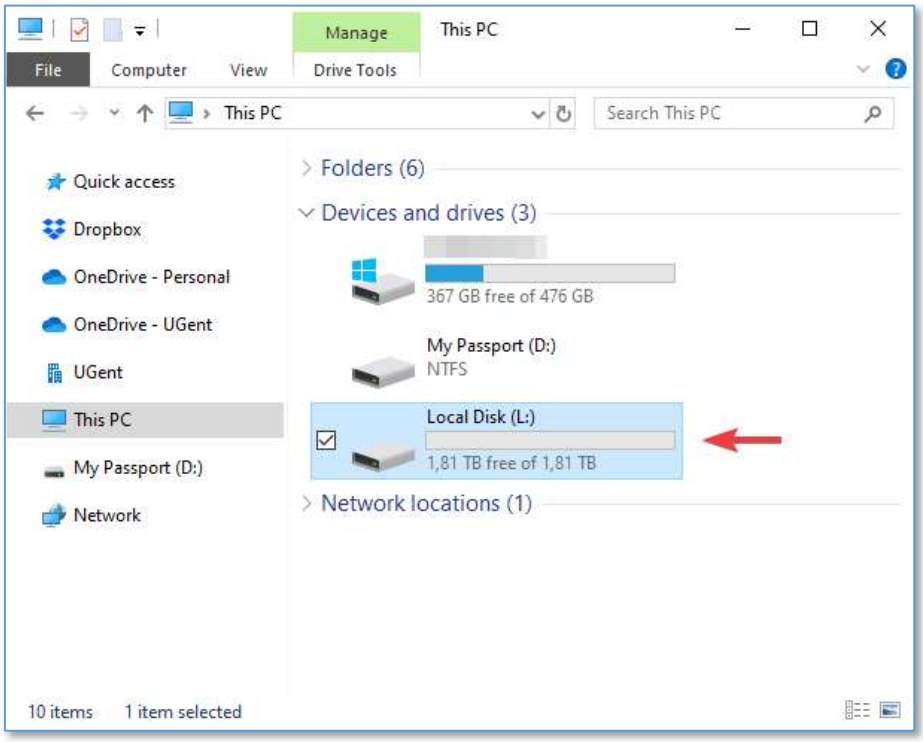
Geef het wachtwoord in en druk op “OK”.

Eens dit is gedaan wordt de versleutelde schijf ontsloten en gekoppeld aan je systeem. Het gevolg is een dat er een nieuwe lokale schijf bij komt op je computer (in dit geval onder de schijfletter L:\).

Als je dit wil kan je nu het venster van VeraCrypt verkleinen of sluiten.

Stap 2 – Gebruiken

Je kan nu gewoon bestanden naar deze lokale schijf schrijven via de Windows verkenner zoals je met een gewone schijf zou doen.



In bovenstaande screenshot zie je dat er in de Windows verkenner twee schijfletters zijn voor de aangesloten versleutelde schijf. De eerste is D:, waar niet naar kan geschreven worden, en de tweede is L: een virtuele schijf die werd aangemaakt door VeraCrypt om je toegang te kunnen geven tot de versleutelde schijf.

Stap 3 – Afkoppelen

Eens je klaar bent met het bovenstaande, dien je de virtuele schijf nog te ontkoppelen. Als je dit niet manueel doet wordt de virtuele schijf automatisch ontkoppeld wanneer je je computer uitzet. Wees je ervan bewust dat zolang je dit niet hebt gedaan, mensen die toegang hebben tot je computer ook toegang hebben tot de (vertrouwelijke) bestanden van de virtuele schijf.

Je gaat als volgt te werk: eerst selecteer je in VeraCrypt de schijf die je wil afkoppelen en vervolgens druk je op “Dismount”. De schijf wordt afgekoppeld en verdwijnt van je systeem.

LICENSE