Privacy & Security Essentials

Encryptie

app VeraCrypt

–

2019 v2

Encryptie – issue bij non encryptie & maatregelen

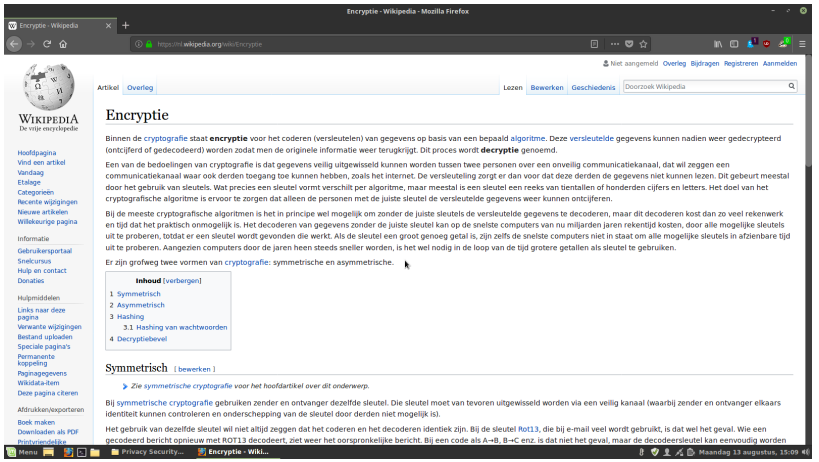
Zeer vele apps hebben machtigingen om bestanden en gegevens te lezen en “er mee te doen wat ze willen”. En sommige web browsers hebben “hidden features” zodat ze ook bij gegevens kunnen. Bekend is ook dat Windows10 via telemetrie zeer veel gegevens van gebruiker upload naar Microsoft servers. Het is van belang dat “indien gewenst” of ingeval van AVG privacy en security noodzaak, bestanden worden beveiligd met encrypty. Voor theoretische uitleg:
→ zie: https://nl.wikipedia.org/wiki/Encryptie

Bedoeling van onderhavige info is geven van “praktische” inzichten en gereedschap (tool – app) om encryptie “cross platform” hanteerbaar te maken bij dagelijkse gang van zaken op PC, iMac, laptop, tablet, chromebook en smartphone.

Praktisch punt is dat bestanden die zijn encrypt door gebruiker altijd weer teruggelezen moeten kunnen worden. Immers, bestanden encrypten is één zaak, maar als het betreffende apparaat waarop de encrypte bestanden fysiek staan niet beschikbaar is door bijvoorbeeld verlies, diefstal, schade of mollest dan is het van belang dat eigenaar van bestanden door middel van de “uiteraard aanwezige fysiek elders opgeslagen” backup de encrypte bestanden op een willekeure andere computer kan recoveren. En is het uitermate handig om ongeacht de computer of OS daarvoor een uniforme app te hebben.

Wat aantal apps voor encryptie betreft zijn er zeer veel mogelijkheden, die vaak gebonden zijn aan een bepaald OS, of niet alle gangbare OS’n afdekken. Om ingeval van een recovery er zeker van te zijn is volgens www-internet techies de consensus dat de app VeraCrypt als meest bertrouwbaar en gangbaar is te beschouwen.

De app Veracrypt ondersteunt verschillende encryptie technieken. In het navolgende wordt uitgegaan van gebruik van:
→ AES SHA-512 | deskundigen zijn het over eens dat er momenteel geen mogelijheid bestaat om deze encryptie te breken.



Encryptie – VeraCrypt: algemeen

Als een niet-encrypted ‘bron’ bestand naar een ‘doel’ encrypted logical file container op eigen interne (local) HDD, eMMC of SSD of naar een ‘doel’ encrypted volume partitie (evt op externe USB drive of SD-card etc) wordt gekopieerd dan wordt automatisch(!) dat bestand encrypted in doel, en blijft de bron niet encrypted achter.

Dat is uiteraard zeer wenselijk bij het maken van een backup of voor “on the go – OTG”. Dus, als gebruiker in bovengenoemd voorbeeld na het plaatsen van het bestand in ‘doel’ verder niets doet dan bestaan er twee versies van bestand, te weten: 1) de leesbare niet encrypted versie in bron en 2) de wel encrypted versie in doel.

Als het in bovengenoemd voorbeeld de bedoeling is dat gebruiker geen backup of OTG maakt, maar de bestanden op de locale hard disk (HDD, eMMC, SSD etc) wil encrypten zodat niemand anders deze ooit kan inzien, dan zal de ‘normaal te lezen” bron handmatig moeten worden verwijderd, tenzij het move/verplaats commando is gebruikt (ipv van copy/kopieer).

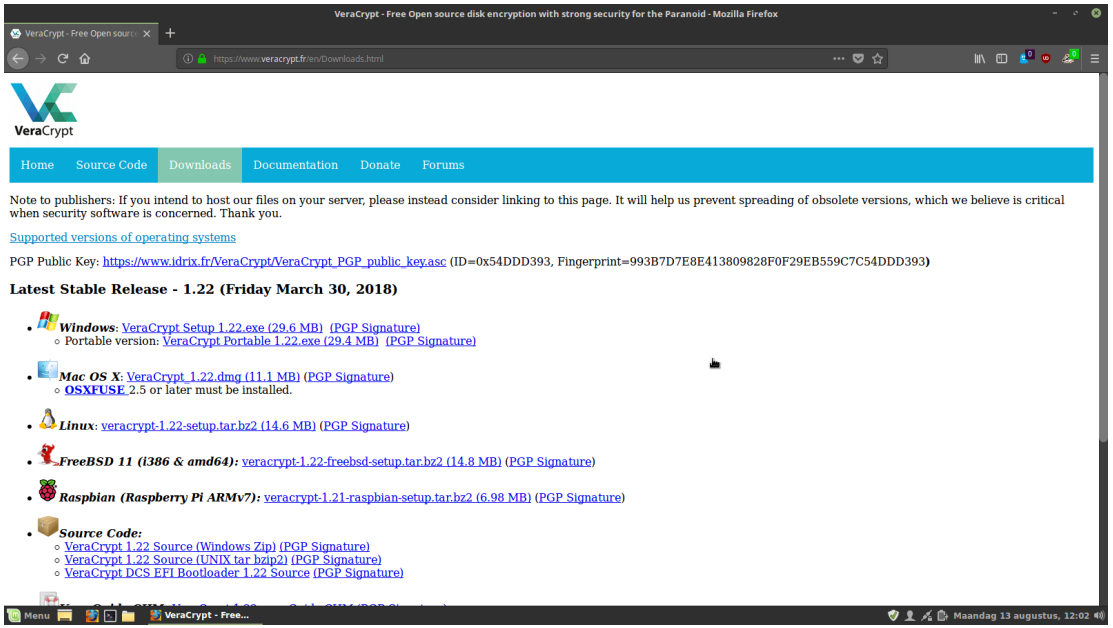
Als een encrypted ‘bron” bestand naar een niet-encrypted ‘doel’ folder wordt gekopieerd dan wordt automatisch(!) dat bestand de-crypted in doel, en blijft bron encrypted achter, tenzij het move/verplaats commando is gebruikt (ipv van copy/kopieer).

VeraCrypt doet niet aan encryptie op bestandsnivo – doet wel bestand(en) gegroepeerd in een VeraCrypt encrypted doel.

Encryptie – VeraCrypt: installatie

Zoals gesteld functioneert de app VeraCrypt “cross platform” oftewel multi platform en kan dus op bijna alle computers worden geinstalleerd. → zie: https://www.veracrypt.fr/en/Home.html.
Voor iOS en Android is er geen app VeraCrypt maar zijn er equivalenten die o.a. de encryptie techniek AES SHA-512 ondersteunen.

DOEN:
Zie voor OS naar keuze betreffende bijlage:
→ D.1 Veracrypt Windows10 handleiding
→ D.1 Veracyrpt macOS handleiding
→ D.1 Veracrypt Linux handleiding
→ D.1 Veracrypt iOS en Android support
→ D.1 Veracrypt Google Chrome support



Encryptie – VeraCrypt: container of partitie

Na start Veracrypt verschijnt 1e scherm (links onder) en kies button “create volume”; dan 2e scherm (rechts onder):

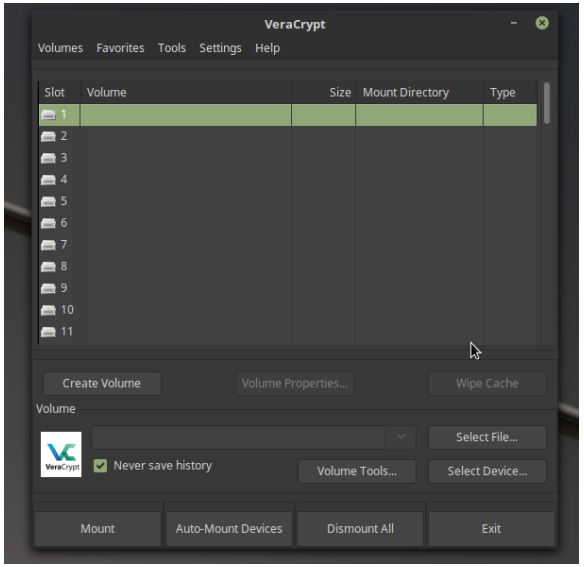
Optie 1: encrypted file container
gebruiker kan in de home folder(of elders naar keuze) een of meerdere(!) file container(s) aanmaken. Een file container is te beschouwen als een folder maar kan niet als een gewone folder worden ingezien door file explorer.

Optie2: volume binnen een partitie of drive
gebruiker kan een deel van de hard disk of drive beschikbaar maken als een volume. Deze volume is te beschouwen als een afzonderlijke partitie op hard disk of usb drive maar kan niet worden ingezien door file explorer.
→ ATTENTIE: zie slide 10 create volume partitie: deze optie (2) is eigenlijk nooit nodig! Optie (1) is simpel en voldoet!

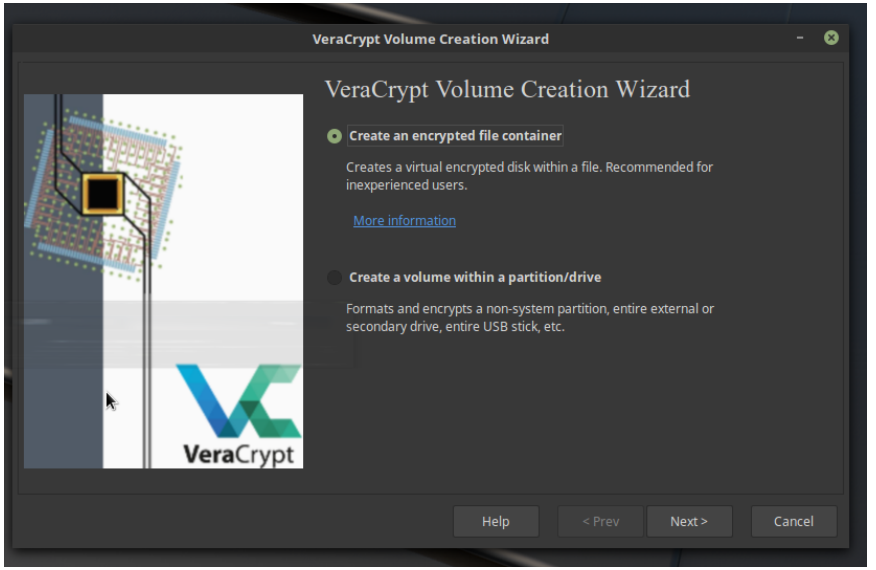
Zodra een bron bestand in doel (1) container of doel (2) volume wordt gezet wordt deze in de doel (1/2) op dat moment encrypt, de bron blijft on-encrypt! – “inzien van bestanden” in een container of volume partitie kan alleen met de (de)encryptie app.

→ optie 1 is aan te bevelen voor dagelijkse gebruik – ook geschikt voor copy naar cloud storage (denk aan #max GB)
→ optie 2 is voor het maken van een backup; of OTG usb drive of SD card (gedeeltelijk) formatteren

DOEN: button “Create Volume”



DOEN: kies optie 1) file container of 2) partitie/drive)



Encryptie – VeraCrypt: standaard of hidden

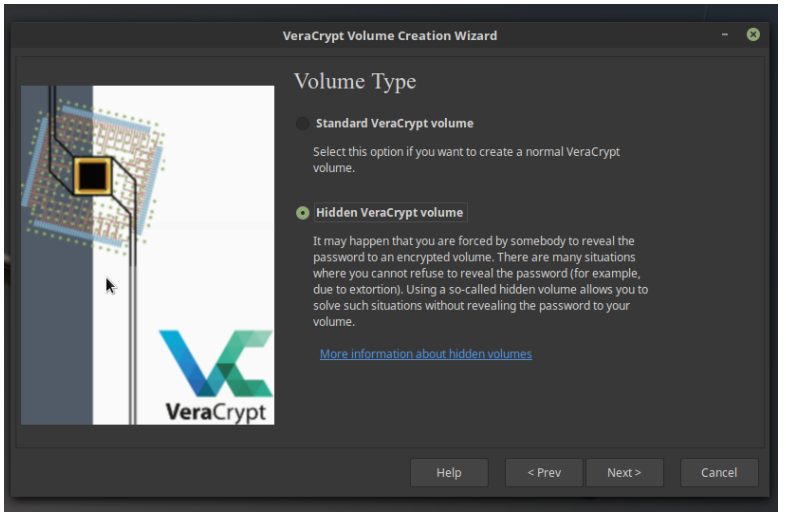
Na keuze (1) file container of (2) de volume partitie verschijnt volgende scherm voor aanmaak met bijzondere kenmerk:

A. Standaard
iedereen die toegang heeft tot het apparaat kan de file container of volume partitie visueel zien vermeld staan bij opstart van file explorer. Maar er verder niet bij/in kan/inzien want password binnen app VeraCrypt is daarvoor vereist.

B. Hidden
in de file explorer is visueel niet te zien of er een file container of volume partitie is. Een onoplettende ‘malversator’ zal niet verder zoeken; een IT’er kent de hidden feature en zal gegevens alsnog snel vinden. Hidden heeft dan ook beperkte functie. Vanwege encryptie kan ‘malversator’ niet bij de gegevens, daarvoor is password vereist.

Keuze
DOEN: standaard (A)

of
DOEN hidden (B):

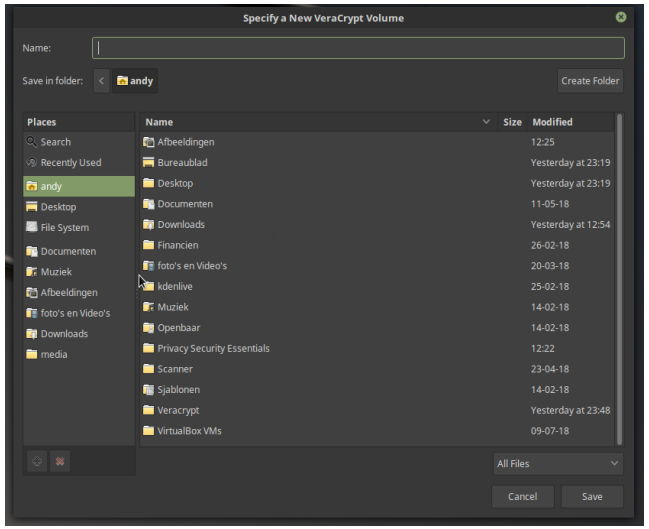


Encryptie – VeraCrypt: volume location

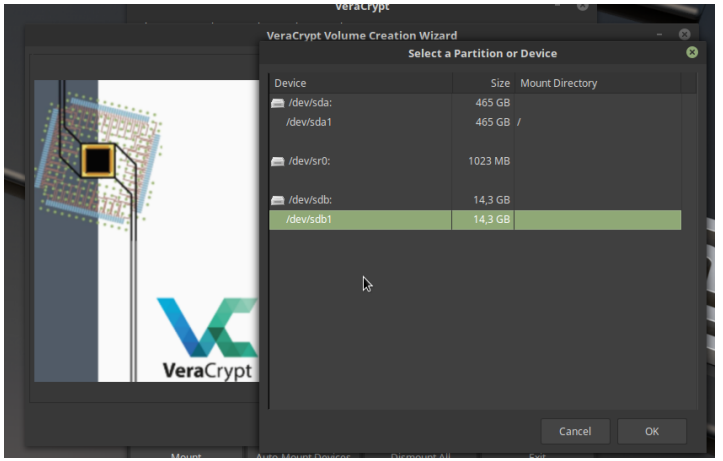
Na keuze 1-A/B encrypted file container verschijnen volgende 2x schermen linker kolom
Na keuze 2-A/B encrypted volume partitie verschijnen volgende 2x schermen rechter kolom

→ let op, er staat “volume” location: die term “volume” geldt bij dit scherm voor zowel keuze 1-A/B als 2-A/B

Keuze 1-A/B:
DOEN: kies locatie in folder structuur



Keuze 2-A/B:
DOEN kies device HDD, eMMC, SDD of extern USB



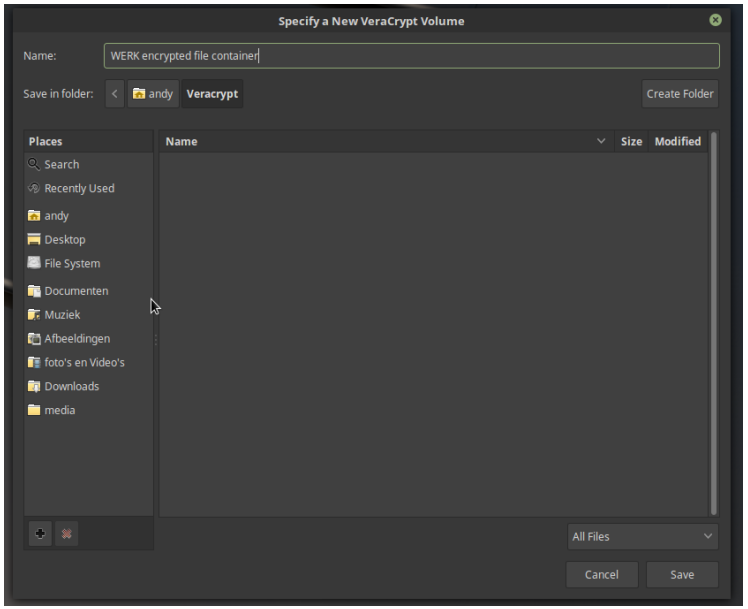
Encryptie – VeraCrypt: aanmaak volume naam

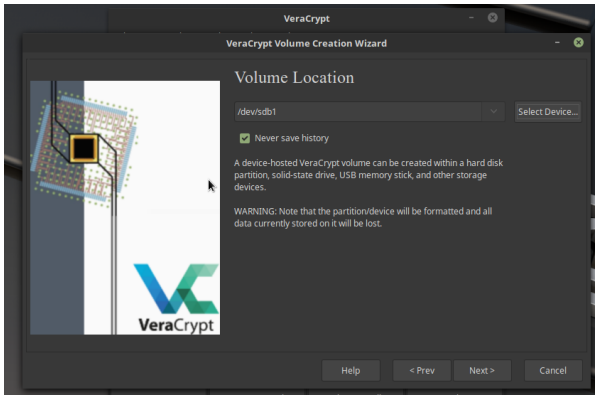
Na keuze 1-A/B file container locatie wordt gevraagd om de naam gewenste nieuwe container.
→ In dit voorbeeld is gekozen locatie /usr/home/andy/Veracrypt, met naam van container:
→ WERK encrypted file container

Zie volgende slides, ten behoeve van voorbeeld ook containers aangemaakt met namen:
→ PRIVE encrypted file container
→ HOBBY encrypted file container
Ter illustratie dat er dus meerdere encrypted containers aangemaakt en gekoppeld (mounted) kunnen worden

Na ingave van locatie en nieuwe naam van container (scherm links onder) wordt bevestiging gevraagd (scherm rechts onder).
→ laat default vinkje aan staan bij “never save history”.

DOEN:
→ bij 1 (A/B) ingave naam van “Container”
→ bij 2 (A/B) bevestig naam van “Device”
→ druk button “Next”





Encryptie – VeraCrypt: volume password en format

Voor beide keuze 1-A/B of 2-A/B geldt dat er wordt gevraagd om volume password scherm (zie links onder). In dit voorbeeld is gekozen voor “password”. Dit is een van de meest gebruikte passwords te wereld en dus niet te adviseren. Dus gebruiker moet zelf een betere kiezen, en die ook goed te onthouden is. Want als gebruiker password vergeet dan zijn de bestanden in de 1) file container of 2) volume partitie voor altijd verloren cq niet meer te recoveren.

Format Options scherm (zie rechts onder) is bepalend in hoeverre de gegevens op ander OS (cross platform / multi platform) gelezen kan worden. En verder bepalend voor maximale bestand grootte. Zo kan FAT een maximaal bestand grootte van 4GB aan. Dat kan belangrijk zijn als bijvoorbeeld gebruiker een MS Outlook *.pst bestand met heel veel mails, en dus groter dan 4GB, encrypted wil opslaan. Of gebruiker wil encrypted video(s) opslaan en één of meerdere daarvan zijn groter dan 4GB. In dat geval kan gekozen worden voor exFAT. Of NTFS format (Microsoft), hetgeen door macOS alleen als “lezen” wordt ondersteund; dat wil zeggen dat op een iMAC de app Veracrypt niet het format NTFS kan formatteren of bestanden daarin kan “(weg)schrijven”, doch wel/alleen “lezen” – bij recovery handig. Linux kan “alle” formats handelen.

Let op: uitleg van “keyfile” is nice to have – doch niet beschreven ter beperking van hoeveelheid informatie op dit moment

DOEN:
→ geef in: password naar keuze
→ kies: Next

DOEN:
→ geef in: keuze
→ skip quick format en kies: Next

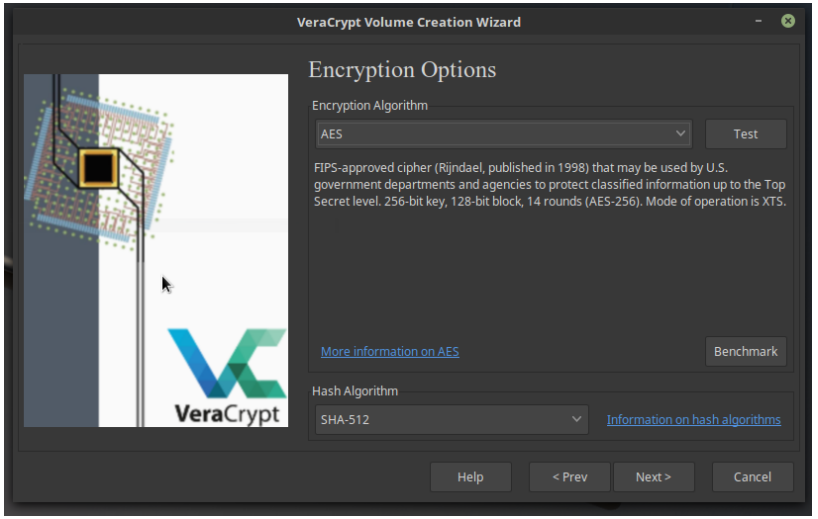
Encryptie – VeraCrypt: encryption options en volume size

Ongeacht de keuze 1-A/B of 2-A/B, wordt gevraagd om encryption options. in dit voorbeeld is gekozen voor:
→ AES, zie: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
→ SHA-512 zie: https://en.wikipedia.org/wiki/SHA-2

Gebruiker kan altijd experimenteren met andere, binnen VeraCrypt, geboden encryptie methode. Echter, wat betreft performance bij dagelijks gebruik en mede gelet op dat “support”-apps niet alle encryptie methoden ondersteunen, is het advies om (zie scherm links onder) in dit voorbeeld gekozen methode “AES SHA-512” te hanteren.

Volume Size scherm (zie rechts onder): ongeacht keuze 1 (A/B) file container of 2 (A/B) volume partitie: de gekozen ruimte wordt tijdens formateren daarvan geheel ingenomen! Dus, overdenk eerst de functie en hoeveel ruimte daarvoor nodig is. Kies niet “te groot” want als ruimte te klein, dan kan altijd een nieuwe grotere aangemaakt worden, en dan de inhoud van “kleine” naar “grotere” worden verplaatst. En wat betreft kopieren naar cloud: overdenk wat de maximale cloudsize is en zorg dat deze niet wordt overschreden door VeraCrypt volume size. Hetzelfde geldt voor usb drive: de VeraCrypt volume size kan usb drive capaciteit niet overschrijden.

DOEN:
→ kies “AES SHA-512”
→ kies Next



DOEN:
→ kies aantal en eenheid (bv: x MB of y GB)
→ kies Next

Encryptie – VeraCrypt: volume password en format

Voor beide keuze 1-A/B of 2-A/B geldt dat er wordt gevraagd om volume password scherm (zie links onder). In dit voorbeeld is gekozen voor “password”. Dit is een van de meest gebruikte passwords te wereld en dus niet te adviseren. Dus gebruiker moet zelf een betere kiezen, en die ook goed te onthouden is. Want als gebruiker password vergeet dan zijn de bestanden in de 1) file container of 2) volume partitie voor altijd verloren cq niet meer te recoveren.

Format Options schemrm (zie rechts onder) is bepalend in hoeverre de gegevens op ander OS (cross platform / multi platform) gelezen kan worden. En verder bepalend voor maximale bestand grootte. Zo kan FAT een maximaal bestand grootte van 4GB aan. Dat kan belangrijk zijn als bijvoorbeeld gebruiker een MS Outlook *.pst bestand met heel veel mails, en dus groter dan 4GB, encrypted wil opslaan. Of gebruiker wil encrypted video(s) opslaan en één of meerdere daarvan zijn groter dan 4GB. In dat geval kan gekozen worden voor exFAT. Of NTFS format (Microsoft), hetgeen door macOS alleen als “lezen” wordt ondersteund; dat wil zeggen dat op een iMAC de app Veracrypt niet het format NTFS kan formatteren of bestanden daarin kan “(weg)schrijven”, doch wel/alleen “lezen” – bij recovery handig. Linux kan “alle” formats handelen.

DOEN:
→ geef in: password naar keuze
→ kies: Next

DOEN:
→ geef in: keuze
→ skip quick format en kies: Next

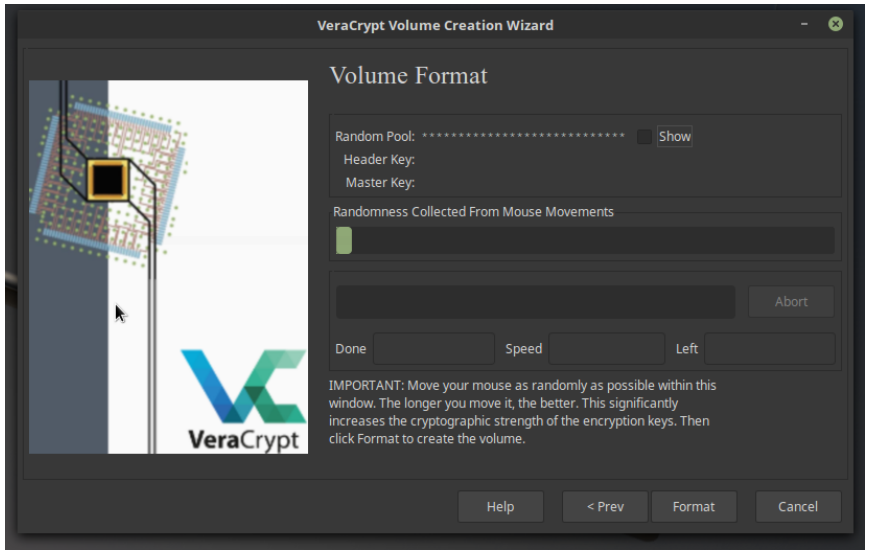
Encryptie – VeraCrypt: volume format

Na ingave van password en volume format uit vorige slide gaat app VeraCrypt daadwerkelijk over tot aanmaak en formatteren van gewenste 1) file container of 2) volume partitie. Scherm (zie links onder) verschijnt en bedoeling is dat gebruiker de muis gedurende een tijdje “random” oftewel “doe maar wat” beweegt. Op scherm 2e balkje wordt tijdens het random bewegen gevuld en als “gereed” druk dan op button “Format”. Zie voor uitleg wat dat random bewegen doet onderaan het scherm bij “IMPORTANT”.

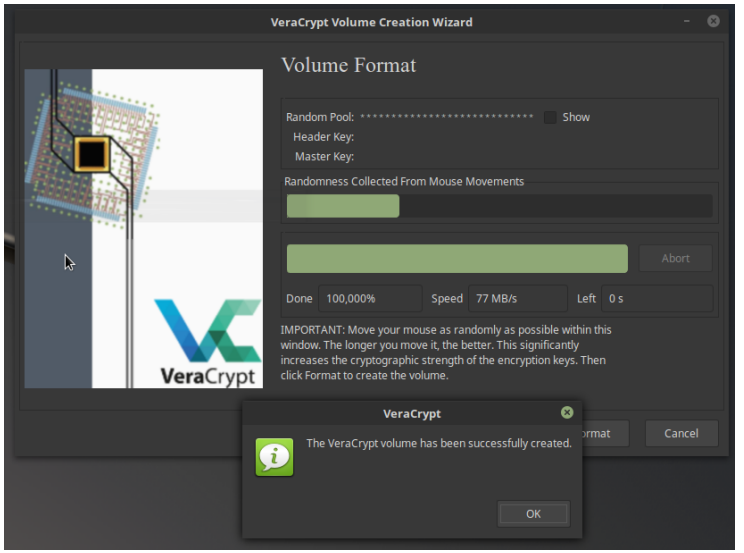
Het formatteren kan naar gelang de grootte van de volume lang duren, maar uiteindelijk verschijnt scherm (zie rechts onder) en de file container of volume partitie is aangemaakt, en geschikt voor gebruik. Dat “gebruik” begint dat app VeraCrypt teruggaat naar 1e scherm (slide 5 vab deze info) en daarin de 1) file container of 2) de volume partitie moet worden aangekoppeld door middel van 1) file container “Select file” of naar keuze 2) volume partitie “Select Device” ; en dan button “Mount”.

→ Attentie: app flow aanmaken is nu “gereed” ; lees verder voor info omtrent gebruik!

DOEN:
→ beweeg muis langdurig
→ kies: Format



DOEN:
→ Druk button: Ok



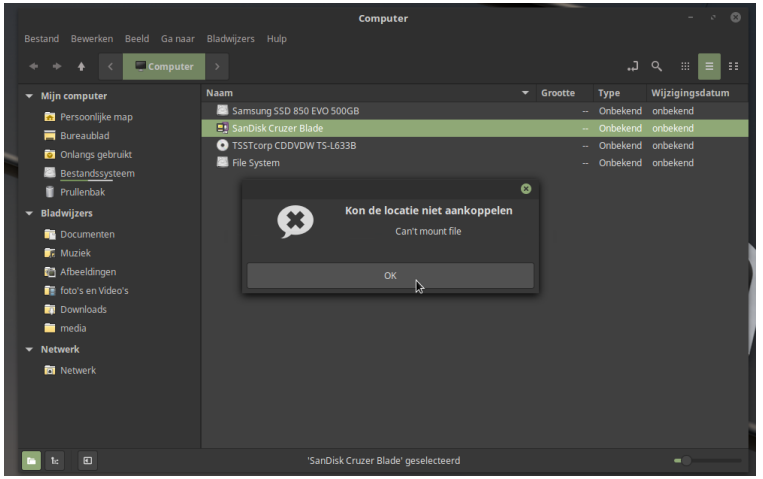
Encryptie – VeraCrypt: gebruik volume partitie

ATTENTIE: bij keuze 2 (A/B) het aanmaken van een 2) volume partitie om bijv. een usb drive geheel, of gedeeltijk, speciaal met de app VeraCrypt te formatteren is eigenlijk niet nodig en niet aan te bevelen! Want: als bestanden in een 1) file container staan, dan kan de file container ‘gewoon’ naar een standaard run-of-the-mill en vers uit de doos usb drive worden gekopieerd.

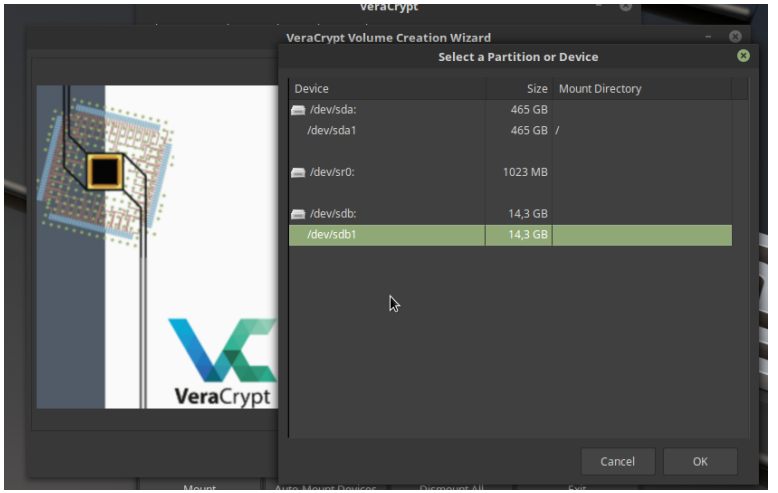
Dan, daarna, bij lezen of recovery van deze (aldus niet speciaal geformatteerde) usb drive verschijnt dan ‘gewoon’ de inhoud, zijnde een bestand cq de 1) file container. In dit voorbeeld zou de inhoud dus kunnen zijn: “WERK encrypted file container. Punt is dat bij aanklikken van dat bestand met file explorer er niks verschijnt want bestand cq container is encrypted.
→ voor lezen (read en write) optie 1) file container is de app VeraCrypt nodig, of een app die dat support.
→ zie slide 18* “gebruik bij backup in cloud” waarbij Google Drive file explorer vergeefs probeert de file container te openen

Indien toch 2 (A/B) gewenst:
volume partitie is te beschouwen als een gebied op hard disk of usb drive dat (standaard of hidden) qua inhoud niet kan worden ingezien door file explorer, daarvoor is app VeraCrypt nodig, of apps die dit ondersteunen “support”. Dus: als op usb drive met optie 2 dit is aangemaakt, dan kan file explorer die usb drive niet aankoppelen, inzien e.d.
→ zie scherm (links onder): aankoppelen cq lezen van een 2) volume partitie zonder benodgde app gaat niet
→ zie scherm (rechts onder): voor lezen optie 2) volume partitie is de app VeraCrypt nodig, of een app die dat support

INFO:
→ usb drive met 2) volume partitie
→ niet te openen zonder encryptie app



DOEN:
→ kies gewenst Device
→ lees bij volgende slide gedeelte over keuze 2)

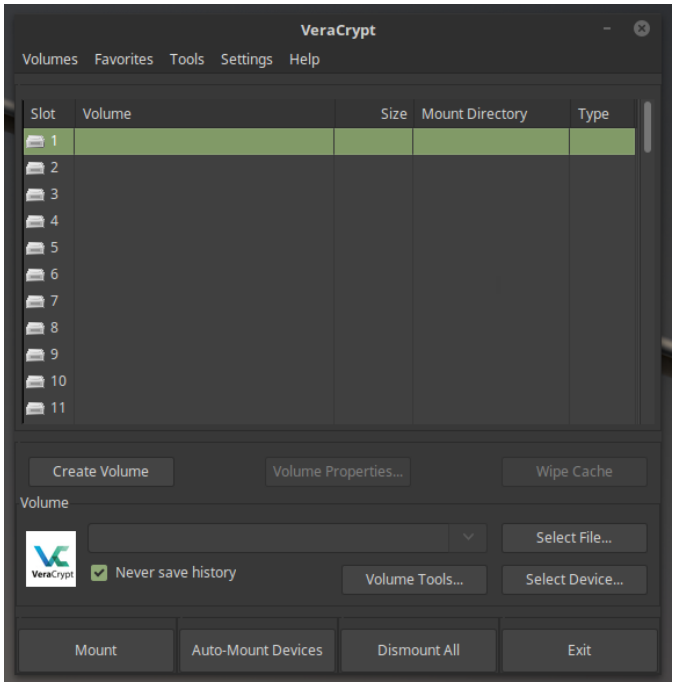


Encryptie – VeraCrypt: start gebruik

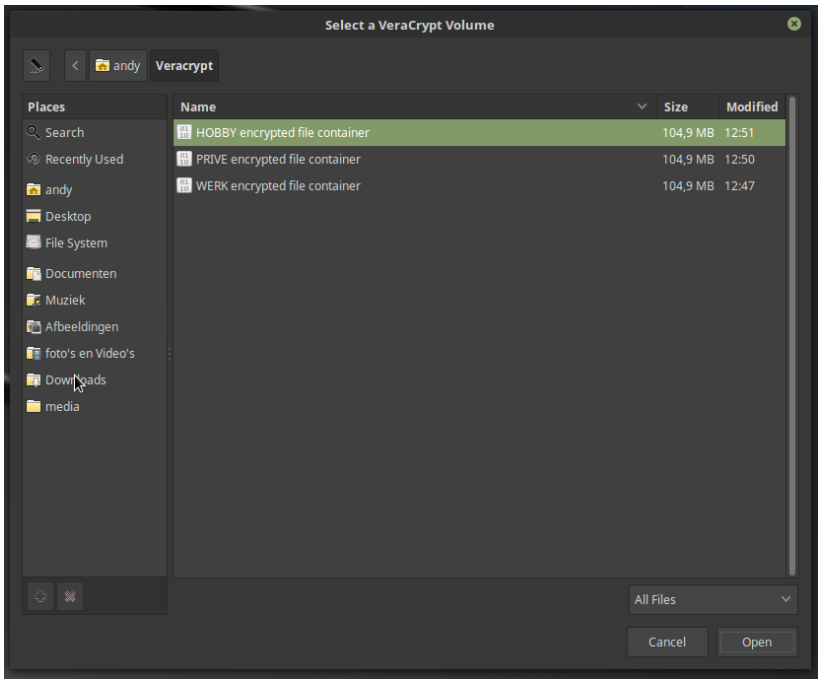
Bij opstart van VeraCrypt, en zie vorige slide: na aanmaak van nieuwe 1) file container of 2) volume partitie, verschijnt scherm (zie links onder) met de keuze om 1 of 2 “te koppelen” voor gebruik. Ter illustratie van mogelijkheden zijn er als voorbeeld 3x file containers aangemaakt, elk 100MB groot met namen WERK-, PRIVE- en HOBBY encrypted file container. De namen bepaalt gebruiker zelf, in dit voorbeel staat in de naam expliciet “encrypted file container” wat is gedaan voor leesbaarheid van info.

Zoals onderstaand te zien zijn er 11x Slots / regels (kan meer zijn als indien gewenst) en bedoeling is dat via muis 1e Slot wordt aangeklikt, die dan groen oplicht. Dan ingeval van 1) druk op “Select File” of ingeval van 2) “Select Device” en de naam van aangewezen file of device wordt presenteerd onderaan scherm (links onder) in vrije ruimte. Dat “aanwijzen” van file of device gaat via automatisiche opstart van “Explorer”; gebruiker navigeert daar doorheen en wijst aan. Als de keuze naar wens is dan druk op button “Mount” en de naam van 1) file container of 2) volume partitie verschijnt ingevuld op de 1e “Slot.
→ dus het hievoor beschreven is 3x gedaan aldus voorbeeld 3x Slots geactiveerd in scherm (zie rechts onder).

DOEN:
→ vul Slot(s) met keuze (1 of 2)



DOEN:
→ Druk button: Open



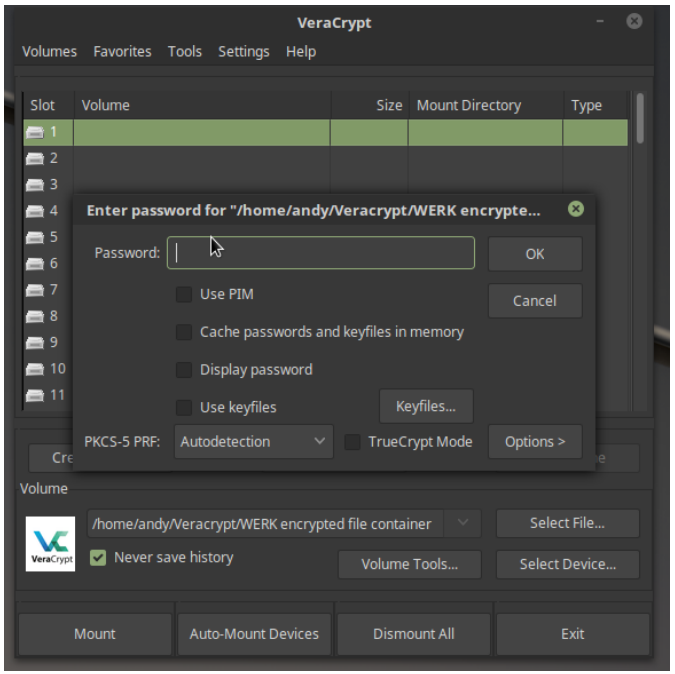
Encryptie – VeraCrypt: gebruik password

Bij openen van een Slot cq daaraan gekoppelde 1) file container of 2) volume partitie verschijnt scherm (zie links onder) met vraag om password van 1 of 2. Als gebruiker het password niet (meer) weet dan is verdere gebruik van 1 of 2 niet mogelijk. Het is dus belangrijk dat gebruiker het eerder, bij aanmaak van 1 of 2, niet(!) vergeet. Dus neem voorzorg maatregelen.

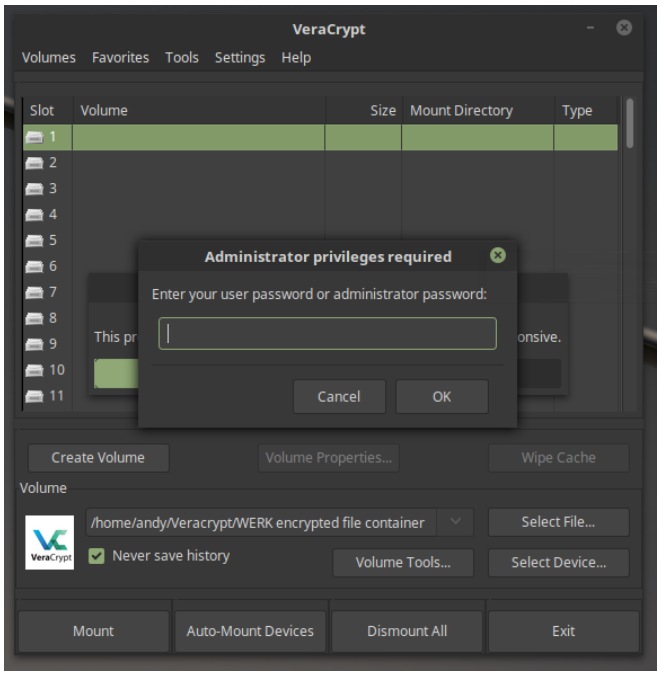
Als gebruiker op computer niet is ingelogd als “Administrator” dan zal er een sub-scherm verschijnen (zie rechts onder) met de vraag om ingave van administrator password. Als gebruiker dat password niet (meer) weet dan is verder gebruik van 1 of 2 wel mogelijk, maar dan op een andere computer waarvan gebruiker wel het password van de administrator weet.

Bij koppelen van meer dan één 1) file container of 2) volume partitie – zoals in deze info als voobeeld 3x Slot ingevuld – dan zal app na 1e opening niet nogmaals om password van administrator vragen.

DOEN:
→ geef in: password (van 1 of 2) en druk: OK



DOEN:
→ geef in: password van adminsitrator en druk: OK



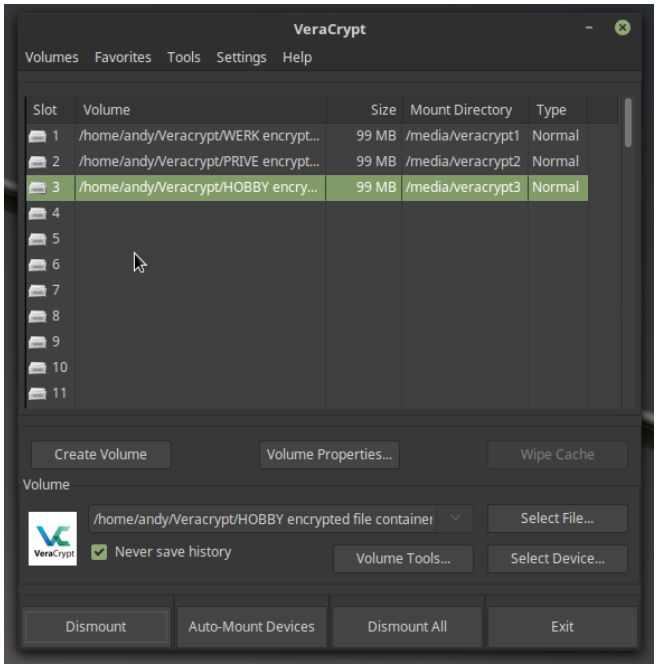
Encryptie – VeraCrypt: gebruik gekoppelde volume(s)

Na juiste password(s) en openen van Slot(s) cq daaraan gekoppelde 1) file container of 2) volume partitie verschijnt scherm (zie links onder) met gewenste “operationele” situatie. Gebruiker kan nu daadwerkelijk bestanden plaatsen, kopieren of verwijderen uit de volume(s).

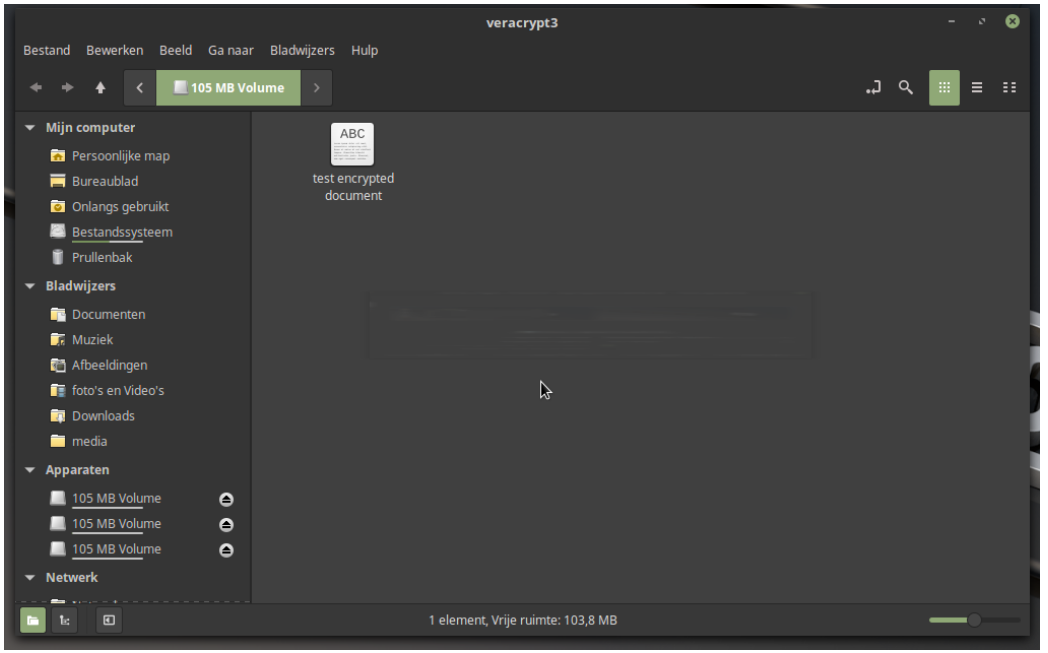
In voorbeeld scherm (zie rechts onder) is Slot 3 geopend en de inhoud daarvan, zijnde 1x voorbeeld bestand, gepresenteerd. De app Veracrypt gedraagt zich gelijk als/aan “File Explorer” waarbij in de linker kolom (van scherm recchts onder) alle folders en devices staan vermeld. En in dit voorbeeld staat in de kop van scherm (zie rechts onder) “VeraCrypt 3”, verwijzen naar 3e Slot cq 3e device uit linker kolom (van scherm rechts onder).

In dit voorbeeld heet het bestand “test encrypted document” wat is aangemaakt met een tekstbewerker. Als gebruiker met muis het bestand aanraakt (en 2x klikt) dan zal automatisch naar gelang de extentie van het bestand, de benodigde app cq in dit geval tekstbewerker opstarten en kan gebruiker verder doen of laten wat gewenst. Dus edit, maar ook copy en move etc.
→ indien gereed dan scherm rechts onder: druk op X sluit venster; dan druk op scherm links onder: Exit; en klaar!

DOEN:
→ geef in: password (van 1 of 2)



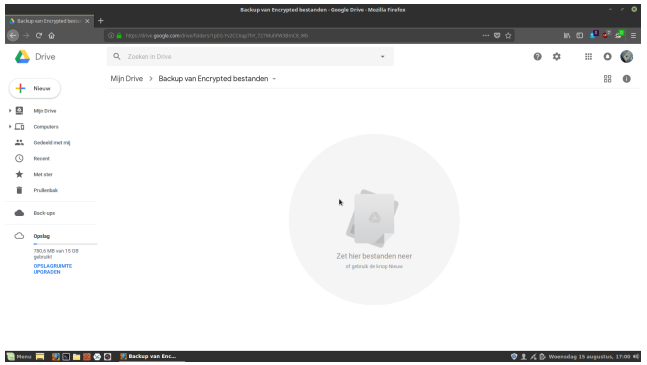
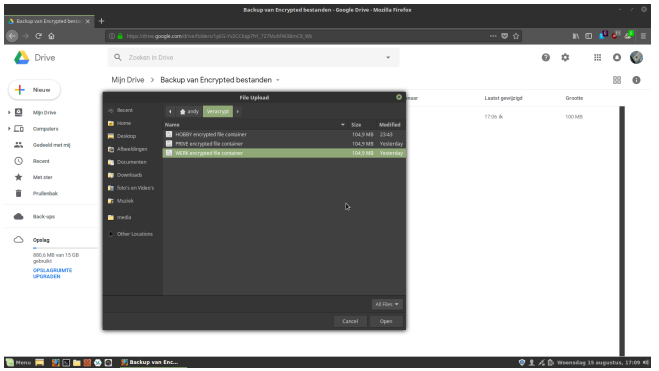
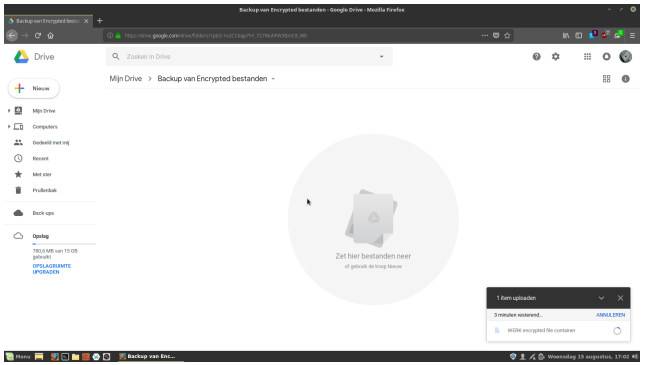
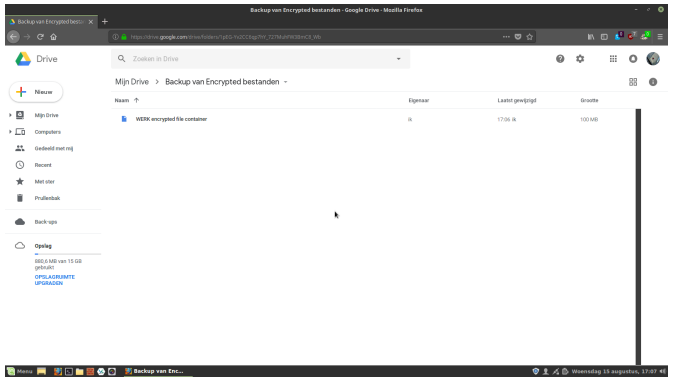
DOEN:
→ geef in: password van adminsitrator

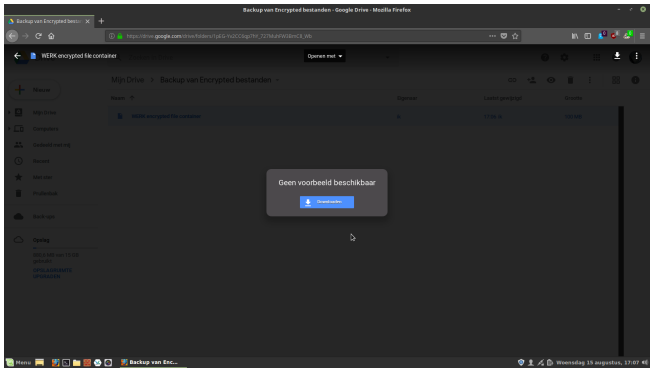


Encryptie – VeraCrypt: gebruik file container backup naar cloud

In begin van deze info is backup of copy van 1) file container naar de cloud. Onderstaande schermen geven chronologisch 1e rij van links naar rechts en dan 2e rij een impressie van te volgen stappen om te komen tot een backup of copy in de cloud.

DOEN:
→ maak aan en/of login via web browser naar cloud, in dit voorbeeld “Google Drive”
→ maak aan een folder, in dit voorbeeld “Backup van encrypted bestanden”
→ ga in die nieuwe folder staan en druk op “Bestand(en) uploaden”
→ de eigen/locale file explorer start; navigeer naar betreffende file container, in dit voorbeeld “WERK encrypted file container”
→ druk op “Open” en het upload proces start, in dit voorbeeld duurt het met 100MB een paar minuten; en gereed!
→ laatste donkere scherm, voorbeeld dat na aanklikken van WERK container “Google Drive” het bestand niet kan lezen



Encryptie – verantwoording

Bronvermelding staat meestal in de screenshots en verder Wikipedia en YouTube

Het www-internet is constant in beweging en feiten en situaties zijn aan wijzigingen onderhevig, daarom:
→ Informatie is van ten tijde van vervaardigen van deze info als vermeld op voorblad – slide 1

TOOLING

Laptop	Acer – Linux Mint
VPN	protonvpn.com
Browser	Mozilla Firefox
Opmaak	LibreOffice
Website	www.summertime.tech