BitLocker onder Linux

Johan Swenker

Onlangs had ik me in de nesten gewerkt op een Windows-computer waarop BitLocker geactiveerd was. Toen ik deze computer dual-boot maakte, ging BitLocker vervelend doen.

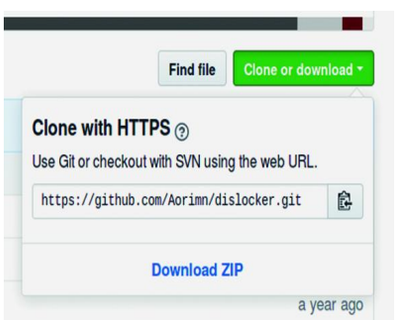
BitLocker eiste bij het booten van Windows de 48-cijferige recovery-key. Nu had ik die gelukkig ooit opgeslagen, dus ik kon bij mijn data. Maar toen ik toch aan het rommelen was, leek het me interessant om te kijken wat je vanuit Linux kunt doen met een disk die met BitLocker versleuteld is.

Dislocker

Een zoekactie met Duck Duck Go naar 'bitlocker linux' gaf me aan dat ik dislocker moest installeren. Ik heb van dislocker geen Debian- of RedHat-package kunnen vinden. De source van dislocker is echter op verschillende plaatsen te downloaden. Uit alle beschrijvingen kreeg ik de indruk dat de versie van Aorimn bij github de originele versie is.
Die versie heb ik daarom opgehaald. Je kunt immers nooit weten of anderen er nog malware, of een taskbar, aan toevoegen.

Github

Ik heb ervoor gekozen om de zip-file op te halen bij
https://github.com/Aorimn/dislocker
Als je wilt kun je ook netjes git gebruiken.



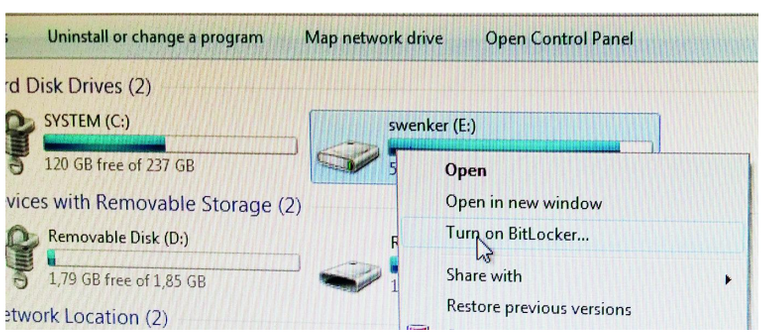
Voordat ik een zip-file uitpak, controleer ik altijd of ze netjes een directory aanmaken, of dat ze domweg alle bestanden in de huidige directory neerzetten. Github maakt mooie zip-bestanden, die je zonder problemen in je home-directory kunt uitpakken.

Het commando:
`unzip ~/Download/dislocker-master.zip`
creëerde netjes de directory-dislocker-master. In het installatie-bestand **INSTALL.md** staat netjes beschreven hoe je dislocker moet installeren.

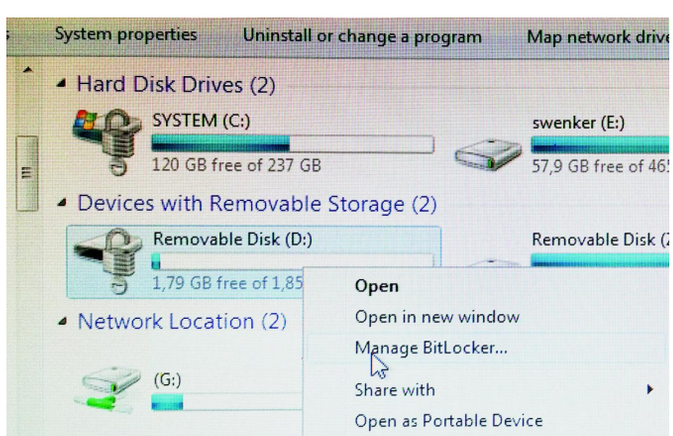
Een belangrijke stap is het installeren van de C-compiler en de bibliotheken voor encryptie. Op mijn Ubuntu 16.04 ging dat met:
`sudo apt-get install gcc cmake make libfuse-dev libmbedtls-dev ruby-dev`

In het installatiebestand staat beschreven hoe dat voor andere Linux-distributies werkt.

Je moet nu eerst het commando `cmake .` uitvoeren (denk om die punt!). Dat commando controleert of je de C-compiler en de bibliotheken geïnstalleerd hebt. Met het commando `make` worden de dislocker-executables gemaakt. Voordat ik ze installeerde, heb ik eerst geprobeerd of ze werken. De dislocker-executables komen in de src-directory terecht en zijn van daaruit aan te roepen. Het echte installeren moet weer met root-rechten. Met `sudo make install` worden de dislocker-executables netjes naar **/usr/local/bin** gekopieerd.



Voor dit artikel heb ik met een Windows-computer een USB-stick van BitLocker voorzien. Op een computer waarop BitLocker beschikbaar is, gaat dit met een rechtermuisklik in de verkenner. Als de USB-stick voorzien is van BitLocker, dan kun je met een rechtermuisklik de BitLocker-configuratie aanpassen. De partitie **/dev/sdc1** is een BitLocker-partitie, met een simpel wachtwoord: *Castor123*. Onder Windows heb ik ook de recovery-key opgeslagen.



Het programma ***dislocker-file*** maakt uit een BitLocker-partitie een heel groot niet-versleuteld bestand. Het commando `sudo dislocker-file -uCastor123 -V /dev/sdc1 cleartext` genereerde een 2 GByte groot bestand met de naam cleartext in de huidige directory. Je hoeft achter `-u` het wachtwoord niet op te geven.
In dat geval vraagt dislocker-file er gewoon om. Ik raakte even in verwarring toen ik een spatie typte tussen `-u` en het wachtwoord **Castor123**: de uitvoer kwam terecht in een bestand met de naam Castor123.

Het bestand **cleartext** is een gewoon NTFS-filesystem, maar dan in de vorm van een bestand. Net als **/dev/sdc1** is **cleartext** alleen te lezen en te schrijven door **root**.
Het standaard mount-commando ontdekt zelf dat het een

NTFS-filesysteem is, en dat het een bestand is. Extra opties zoals `-t ntfs` en `-o loop` zijn dus overbodig. Met `sudo mount cleartext /mnt` komt de inhoud van **cleartext**, en dus de onversleutelde inhoud van **/dev/sdc1**, beschikbaar in de directory **/mnt**. Het unmounten gaat met `sudo umount /mnt`.

Het voordeel van dislocker-file is meteen ook het nadeel: er wordt een onversleutelde kopie van de oorspronkelijke versleutelde partitie gemaakt. Er kan dus niets misgaan met de oorspronkelijke data, maar het kost heel veel schijfruimte.

Het programma dislocker-fuse doet ogenschijnlijk hetzelfde als dislocker-file, maar het verschil is dat het aangemaakte bestand niet echt bestaat. Een beetje zoals de bestanden in **/proc en /dev/**; ook díe ontstaan pas als ze opgevraagd worden.

Voordat we dit kunnen gaan uitproberen, moeten we eerst twee directories maken: `sudo mkdir /mnt/X` en `sudo mkdir /mnt/Y`

Met het commando:
`sudo dislocker-fuse -p158521-532642-261118-227117-341176-602052-466873-564025 -V /dev/sdc1 /mnt/X`
wordt nu in **/mnt/X** een pseudo-bestand 'dislocker-file' aangemaakt. Ik heb er hierbij voor gekozen om de recovery-key te gebruiken die ik met knippen en plakken opgegeven heb. Als je de recovery-key moet overtypen van een papiertje, dan moet je de optie `-p` geven zonder recovery-key. Dislocker zal dan om de key vragen, en deze controleren op typfouten tijdens het intypen.

Het pseudo-bestand kunnen we mounten met:
`sudo mount /mnt/X/dislocker-file /mnt/Y`.

Indien gewenst kun je bij dislocker-fuse de optie `-r` opgeven, dan is het pseudo-bestand read-only. Je kunt de onderliggende partitie **/dev/sdc1** dan niet per ongeluk beschadigen.
Indien gewenst kun je bij `mount` de optie `-o ro` opgeven. Deze optie zorgt ervoor dat het gemounte filesysteem read-only wordt.
Het stoppen van **dislocker-fuse** gaat in twee fasen. Eerst moet met `sudo umount /mnt/Y` het pseudo-bestand ontkoppeld worden van **/mnt/Y**.
Daarna moet met `sudo umount /mnt/X` de partitie **/dev/sdc1** van de USB-stick ontkoppeld worden van het pseudo-bestand.

libbde-utils

Nadat ik bovenstaande allemaal bedacht en beschreven had, heb ik toch nog eens aan mijn Ubuntu 16.04 gevraagd of die iets met BitLocker kan: `apt-cache search bitlocker`.
En zowaar, ***libbde-utils*** komt te voorschijn als ***Tools to access the BitLocker Drive Encryption format***. Na installatie met `apt-get install libbde-tools` heb ik twee nieuwe commando's: `bdeinfo` en `bdemount`.

Het commando `sudo bdeinfo /dev/sdc1` geeft informatie over de versleutelde partitie. Dit commando geeft een stuk minder informatie dan `dislocker-metadata`, maar is daardoor wel beter te gebruiken.

Het commando `bdemount` is vergelijkbaar met `dislocker-fuse`. Ook `bdemount` maakt een pseudo-bestand aan.
Bij `dislocker-fuse` kun je ervoor kiezen of het pseudo-bestand read-only is of dat het veranderd kan worden.

Het commando `bdemount` kan alleen een read-only bestand aanmaken. Dat is heel veilig. De versleutelde partitie kan niet per ongeluk gewijzigd worden. Maar het kan ook niet als je het toch zou willen.