Une méthode de sauvegarde des documents y compris les photographies

Guillaume Marty

Décembre 2020[1]

Table des matières

1 Introduction

La sauvegarde des données est une des choses les plus élémentaires en informatique. Malheureusement, cette étape n'est que peu mis en œuvre dès le début du travail sur un ordinateur de façon générale ; la majeure partie des personnes se dit que la sauvegarde sera faite quand le temps se présentera. Et finalement, c'est là que le problème arrive. Je vois actuellement trop de personnes sur les réseaux sociaux écrire qu'ils ont perdu 4 ans de données car ils n'ont pas eu le temps de sauvegarder quand le disque commençait à lâcher, donc trop tard. La sauvegarde est un processus faisant partie intégrante de celui d'un photographe. On ne le lit que peu de fois. C'est ce qui m'a décidé à écrire ce petit recueil où j'explique une des façons de faire, la mienne. Il n'existe pas de manière universelle. Ce choix a été dicté par mes convictions open source donc sous GNU/Linux et on ne va pas le cacher par un prix réduit par rapport aux solutions toutes prêtes.

Disque dur externe, SSD, NAS, clé usb, Cloud ; tant de mots pour faire cette sauvegarde tant importante, il est certain que cette avalanche de supports de données coûtera une certaine somme. Oui, mais quel est le prix des données, des documents, mais aussi des photos de voyage, de famille, les projets personnels et même professionnels pour certains ? Il me semble que la valeur est inestimable et que cela vaut certainement cette somme pour sécuriser les données et le flux de travail.

Cette partie se cantonnera aux données de darktable et à la bibliothèque de photos. Ce sont juste des données et ces informations pourront être aisément transposées à d'autres types de données, documents par exemple. J'utilise la même méthode pour sauvegarder mes documents,

2 Théorie

2.1 Règle des 3-2-1

Ce nom définit les 3 principes afin de n'avoir peu sinon aucune perte de documents.

Il s'agit donc d'avoir :

— 3 copies minimum
— sur au moins 2 supports physiques différents
— dont 1 dans un endroit physique différent

Et cela pour plusieurs raisons.

Les endroits différents permettent de ne pas mettre les œufs dans le même panier. Un sinistre (incendie, vol...) ne détruira qu'un seul support physique. Au sujet des supports physiques, il existe une attention particulière à avoir. Il faut faire attention à utiliser des supports qui ne sont pas de la même série de fabrication. En effet, si il y a un défaut, il est fort probable que son jumeau sera atteint du même problème tôt ou tard. Dans ce cas, ces deux supports seront caduques.

2.2 Le chiffrement

Dans cette règle des chiffres, il manque l'accessibilité des données surtout dans le cas d'un support amovible. Si vol, la clé ou disque dur sera accessible

en lecture et les documents seront visibles.

Le chiffrement du support sert à protéger l'accès à ces données. Suivant chaque personne, il y aura toujours parmi les photos une partie de personnelle. Cette protection est donc des plus essentielles.

2.3 Type de sauvegarde

2.3.1 Sauvegarde complète

Tous les fichiers et dossiers sont copiés sur un autre emplacement, il s'agit donc d'une copie complète. Ce type de sauvegarde a pour effet de mobiliser beaucoup de mémoire si il s'agit de données nécessitant d'être versionnées. Pour autant, il s'agit d'un type de sauvegarde facilitant la restauration si incident.

2.3.2 La sauvegarde incrémentale

Elle débute par une sauvegarde complète. Ensuite, elle sauvegarde les changements, modifications entre chaque version datée. De ce fait, elle est assez rapide à réaliser (cela dépend des changements depuis la dernière sauvegarde) et ne prend pas beaucoup de place. Cependant, elle est plus longue à restaurer étant qu'il faut remonter dans le temps.

2.3.3 La sauvegarde différentielle

De même que le type de sauvegarde précédente, elle débute par une sauvegarde complète. Par contre, chaque sauvegarde enregistre les modifications depuis la première sauvegarde et non la précédente. De ce fait, elle prend plus de place que le type précédent mais elle est plus rapide à remettre en place.

2.3.4 Sauvegarde uni-directionnelle ou bi-directionnelle

Il s'agit du sens de direction de la sauvegarde. Ce fait est surtout conditionné par la présence d'une ou de plusieurs stations de travail pour, entre autre, la photographie.

Dans le cas d'une seule station de travail, la sauvegarde uni-directionnelle suffit. En effet, la sauvegarde doit simplement s'effectuer du poste de travail vers le support de sauvegarde. Ce n'est que dans le cas d'une restauration que la direction sera inversée. Cette situation sera normalement rare.

Si l'on possède plusieurs stations de travail, la sauvegarde uni-directionnelle sera trop compliquée à gérer. La seconde option est la plus pertinente. La sauvegarde se fera dans les deux sens en prenant en compte les dernières informations en terme d'ancienneté.

2.3.5 Sauvegarde manuelle ou automatique

Ce qui compte dans la sauvegarde, c'est de la faire. Il ne s'agit pas de dire que l'on va la faire en programmant un alinéa dans une todo-list que l'on va reporter... La différence entre ces deux manières est le facteur humain qui est faillible. Il suffira d'une seule fois où l'on se dira qu'il est possible de faire cela le lendemain, mais entre temps, le disque aura rendu l'âme sans avoir pu effectuer de sauvegarde. Il est donc primordial d'automatiser au maximum le processus.

2.4 Type de données pour la photographie et sauvegarde

Lorsque l'on considère la photographie et donc aussi darktable, il existe deux types de données :

— la photographie en tant que tel : le format brut raw
— la base de données que ce soit celle de darktable au sont stockées les préférences mais aussi les développements ainsi que le fichier xmp dans le dossier physique

La première n'a pas de nécessité à sauvegarder les anciennes versions. Cela pourrait s'entendre avec le fichier xmp, cependant il n'apparaît pas que le développement soit une priorité à être enregistré. Ce sont les clichés les plus importants. Une chose est aussi à prendre en compte ; versionner c'est-à-dire sauvegarder les versions prend de la place. Lorsque la carte mémoire est déchargée sur le pc, une première sauvegarde doit être faite pour sécuriser les données. Puis, un premier tri se fait, un deuxième et un troisième qui vont diminuer le nombre de clichés qui seront gardés. Dans le cas d'une sauvegarde simple, la taille de la bibliothèque diminuera ce qui est un bon point. Par contre, dans le cas d'un versionning, la taille sera beaucoup plus importante. Le premier argument est donc la taille. L'autre question peut être : est-il nécessaire de penser "je vais garder les photos non nettes au cas où" ? Il ne semble pas nécessaire de garder tous les clichés nettes ou mêmes ceux issus d'une rafale qui sont à 90% les mêmes. Pour ces différentes raisons, la sauvegarde simple pour la bibliothèque est suffisante.

Par contre, la sauvegarde des anciennes versions de la base de données a entièrement sa place et ceci pour deux raisons :

— garder en mémoire les différentes préférences lorsque l'on manipule un peu trop les options pour pouvoir revenir en arrière
— sauvegarder les préférences lorsqu'il s'agit de revenir sur une version antérieure de darktable. En effet, avec les montées en version de darktable, des mises à jour de la base de données peuvent être faites. La nouvelle version de la base n'est donc plus compatible avec la version antérieure de darktable. Un intérêt est donc de sauvegarder à chaque montée en version pour pouvoir rétrograder la base de données si la nouvelle version de darktable contient des bugs. Cette raison est d'autant plus valable avec l'utilisation de la version de darktable en développement où les bugs sont nombreux.

3 Logiciels utilisés

Ils sont au nombre de trois dont un sert à automatiser. Ils permettent, à mon sens, de tout faire en ce qui concerne la sauvegarde.

3.1 unison

3.1.1 Avantages

Ce logiciel existe sous GNU/Linux et en ligne de commande.

Il permet de sauvegarder sur un autre média le dossier ou le disque dur en entier. Il fonctionne aussi via le réseau. La sauvegarde est bi-directionnelle et se fera donc dans les deux sens. Étant donné de qui peut le plus peut le mieux,

dans le cas d'une seule station de travail, il fera très bien le travail. Dans ce contexte par rapport à rsync, il a deux avantages :

— il n'utilisera pas l'utilisateur administrateur
— il a une fonction de contrôle. Si la ligne de commande le précise, unison cherche si le fichier est présent sur les deux disques. Si un média est un disque externe et qu'il n'est pas branché, le fichier ne sera pas présent sur un des deux médias. La sauvegarde ne se fera donc pas et les données ne seront pas détruites. Que ce soit sur un disque externe ou non, ce fichier de contrôle devrait, à mon avis, être tout le temps présent.

3.1.2 Installation

Il doit être présent dans les dépôts de la distribution. Sur Debian, un

Listing 1: Ligne de commande

```
sudo apt install unison
```

Il faut noter qu'il doit être installé sur les deux ordinateurs.

3.1.3 Utilisation

Unison s'utilise très simplement :

Listing 2: Ligne de commande

```
unison chemin1 chemin2 -options
```

Comme il n'est pas pratique de devoir tout taper même si c'est mis dans un fichier script, il existe des profils (.prf dans le dossier .unison du répertoire utilisateur) qui seront appelés via une commande plus simple :

Listing 3: Ligne de commande

```
unison profil
```

Ces profils contiendront les chemins des médias ainsi que les options. Il sera donc plus simple de les lancer en automatique ou manuel

3.1.4 Profils

Fichier exemple Voici un exemple :

Listing 4: Fichier profil disque-usb.prf

```
\# repertoire local
root=/home/boum/Documents-heavy/
\# repertoire distant
root=ssh://boum@pi//home/boum/dd/Documents-heavy/

ignore= Path lost+found
ignore= Path .Trash-1000

mountpoint=nas-heavy.md
```

```
force=newer
times=true
batch=true
```

La synchronisation va se faire entre les deux dossiers précisés par les deux chemins. Elle va ignorer les dossiers perdus et retrouvés ainsi que la corbeille. La commande vérifiera la présence du fichier de contrôle (mountpoint). Les options précises sont :

- moutpoint= spécifie le fichier qui sera vérifié ; si il est présent sur les deux médias, la sauvegarde est lancée
- force=newer : forcer à ne conserver que la version la plus récente à utiliser avec
- times=true : pour synchroniser les dates
- batch=true : pour automatiser les synchronisations sans une seule confirmation manuelle pour l'automatisation

Et pour le lancer, ce sera

Listing 5: Ligne de commande

```
unison disque-usb
```

Il existe bien sûr d'autres options que je n'utilise pas, celles-ci suffisent amplement à la tâche voulue.

3.1.5 Conclusion

Ce logiciel est parfait pour faire des copies miroirs. Dans le cas de plusieurs stations de travail, si le pc 1 change le dossier1 et le pc le dossier2, unison va propager les modifications du disque 1 (dossier1) sur le disque 2 et les modification du disque 2 (dossier 2) sur le disque 1 dans le même temps. Il sera donc utilisé dans le cadre de la sauvegarde des photos.

3.2 borg

3.2.1 Avantages

Passons tout de suite les avantages de geek ; comme les autres, il existe sous GNU/Linux avec la ligne de commande.

Les archives sont chiffrées lui conférant un avantage lorsque la destination n'est pas chiffrable aisément. Elles sont aussi compressées ce qui permet que la taille soit tout de même contenue même dans le cas des sauvegardes versionnées.

Une sauvegarde interrompue pourra être reprise dans un second temps.

Le dernier avantage est que chaque sauvegarde est comme un média externe. Elles peuvent être montées comme une clé usb.

3.2.2 Installation

Il doit être présent dans les dépôts de la distribution. Sur Debian, un

Listing 6: Ligne de commande

```
sudo apt install borgbackup
```

A noter qu'il doit être installer sur les deux ordinateurs.

3.2.3 Utilisation

Préparer le répertoire (repo) */repo* désigne le répertoire où vont être sauvegardées chaque version (*archive*)

Il faut initialiser le répertoire de destination :

Listing 7: Ligne de commande

```
borg init --encryption=repokey-blake2 /repo
```

L'initialisation sera faite avec un chiffrement sur mot de passe. Ils peuvent être locaux ou distants.

Pour réaliser une archive (sauvegarde à un temps T), la commande sera :

Listing 8: Ligne de commande

```
borg create /repo::{now} /source
```

Il est possible de donner un autre nom à l'archive que la date et heure à la place donc de *now* mais cette façon permet de s'y retrouver en terme d'ancienneté.

La compression peut être rajoutée :

— lz4 pour légère
— zlib pour moyenne
— lzma pour maximale

Pour ma part, j'ai choisi lzma avec une compression maximale à 9, soit la commande suivante :

Listing 9: Ligne de commande

```
borg create --compression lzma,9 /repo::{now} /source
```

Lister les archives

Listing 10: Ligne de commande

```
borg list /repo
```

Visualiser une archive Une archive se monte comme une clé usb dans un répertoire avec la commande :

Listing 11: Ligne de commande

```
borg mount /repo dossier
```

Les archives seront accessibles dans le dossier nommé *dossier* dans l'exemple précédent.

Elle se démonte avec :

Listing 12: Ligne de commande

```
borg umount archive
```

Nettoyer les archives Il peut être nécessaire de supprimer des archives selon les besoins. Dans le cadre d'un versionnage de fichiers de configuration, il est possible de supprimer les sauvegardes anciennes lorsque celles-ci sont trop vieilles.

Par exemple, cette commande :

Listing 13: Ligne de commande

```
borg prune -v --list --stats --keep-daily=6
--keep-weekly=6 --keep-monthly=6 /repo
```

va garder un backup par jour sur les 6 derniers jours, 1 par semaine sur les 6 dernières semaines et 1 par mois sur les 6 derniers mois. Il existe bien sûr d'autres conditions.

Il est possible de supprimer un backup précis en spécifiant le nom :

Listing 14: Ligne de commande

```
borg delete /repo::nom-archive
```

Vérifier l'intégrité des backups

Listing 15: Ligne de commande

```
borg check -v --progress /repo
```

3.2.4 Conclusion

Ce logiciel est parfait pour certains usages notamment dans la photographie et darktable. Il assure une sauvegarde des base de données antérieures et permet de récupérer très rapidement une productivité sous darktable lorsque la mise à jour est buguée. Couplé à des routines cron, il fait ce travail de sauvegarde de façon automatique sans avoir à toucher quoi que ce soit.

3.3 crontab

Ce n'est pas à proprement parler un logiciel de sauvegarde. Il est présent dans la liste pour automatiser les sauvegardes. Il lance à la préférence de l'utilisateur une commande, soit toutes les heures, à 19h35 les mardis, jeudis et samedi...

Tous les logiciels précédemment présentés sont utilisables en ligne de commande et donc pleinement compatibles avec cron. Il faudra donc réfléchir et choisir à quelle fréquence lancer quel type de sauvegarde.

Il est normalement installé de base sur une distribution GNU/Linux. Attention, l'édition du fichier crontab se fait dans un terminal. Il s'effectue à l'aide de la commande *crontab* avec ses arguments.

Listing 16: Ligne de commande

```
crontab -l
```

permet de voir les actions que va effectuer cron.

Listing 17: Ligne de commande

```
crontab -e
```

permet d'éditer le fichier de l'utilisateur.

3.3.1 Syntaxe de crontab

La syntaxe est très précise, un peu ardue au départ à comprendre. Chaque ligne est dédiée à une tâche. Elle comprend 6 groupes de caractères. Les 5 premiers spécifient le temps et le dernier la commande à exécuter.

Le temps est défini par ces 5 groupes de caractères :

1. pour minute (de 0 à 59)
2. pour heure (de 0 à 23)
3. pour le jour du mois (de 0 à 31)
4. pour le mois (de 1 à 12)
5. pour le jour de la semaine (de 0 pour dimanche à 6 pour samedi)

A chaque place peut-être spécifié la donnée de temps exacte ou plusieurs en séparant par des virgules, des intervalles avec le trait d'union ou des répétitions avec */X* (X désigne un chiffre) ou tous avec *.

Des exemples seront plus parlants :

Listing 18: Ligne de commande

```
00 */12 * * * unison profil
```

lance la commande de sauvegarde toutes les 12 heures et ce tous les jours.

Listing 19: Ligne de commande

```
30 1-5 * * 2 unison profil
```

lance la sauvegarde les mardis toutes les heures de 1h30 à 5h30.

Vous trouverez plein d'autres exemples sur la toile.

3.4 syncthing (bonus)

Il me sert à enregistrer sur mon ordinateur les photos de mon smartphone. Avec celui-ci, cette partie se fait automatiquement. Il ne restera plus qu'à copier les photos dans le bon dossier des photographies. Comme ce n'est pas un logiciel indispensable, je ne m'attarderais que peu dessus.

L'installation doit se faire sur les deux terminaux (smartphone et ordinateur). Un tutoriel comprenant toutes les étapes se trouve sur cette page.

Quelques précisions pour que l'installation et la configuration se passent pour le mieux :

— utiliser le QR code pour ajouter la machine sur le smartphone est la manière la plus facile. Ensuite attendre l'autorisation sur l'ordinateur.

— ne pas oublier de lancer le démon syncthing sur les deux machines. Il ne se lance pas automatiquement.

4 Matériel

L'ensemble est composé au minimum de deux ordinateurs de type raspberry pi. L'un est un raspberry pi zéro W et l'autre un raspberrypi 3B+. Le premier sert de sauvegarde versionnée pour les documents mais surtout la base de données de darktable et le deuxième de NAS (Network Attach Storage). Le gros avantage est la consommation de courant très limitée et le coût assez limité.

Cette partie va se concentrer sur l'installation de ces deux mini-pc.

4.1 Raspbbery pi zéro W

Il est vraiment petit et peut se faufiler de partout. Il va donc servir de sauvegarde via borg. Le chiffrage sera implémenté par ce logiciel.

4.1.1 Installation

Ce petit objet ne sera accessible que via ssh, c'est-à-dire en ligne de commande. Il est donc seulement nécessaire de lui installer un système minimal comme Raspberry Pi Os Lite.

Carte sd Les étapes sont :

- Télécharger la dernière version de raspberry pi OS : version Lite
- Décompresser le zip
- Lancer l'installation sur la carte sd sous bash avec dd :

Listing 20: Ligne de commande

```
sudo dd bs=4M if=fichier.img of=/dev/sdb conv=fsync
```

Attention à bien sélectionner le fichier source mais surtout le périphérique de sortie et ceci afin de ne pas effacer le disque du système. La ligne précédente n'est qu'un exemple, c'est à adapter à votre configuration !

- activer l'accès à distance ssh en créant un fichier nommé ssh dans le volume boot ; dans le bon répertoire un *touch ssh* fait l'affaire, le fichier peut être vide
- activer le wifi avec un fichier wpa.supplicant.conf sur le volume boot contenant

Listing 21: wpa.supplicant.conf

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
country=FR

network={
  ssid="SSID"
  psk="PASSWORD"
  key_mgmt=WPA-PSK
  scan_ssid=1
}
```

Changer les termes entre guillemets en les modifiant par les bons paramètres de votre installation.

La carte sd est maintenant à insérer dans le Rpi.

Premier démarrage Mettre le rpi sous tension avec la carte SD branchée. Laisser du temps avant de vous brancher en ssh.

Listing 22: Ligne de commande

```
ssh pi@raspberrypi
```

Le mot de passe est raspberry.

Il est nécessaire de changer des paramètres pour sécuriser le raspberry pi avec l'utilitaire raspi-config.

Listing 23: Ligne de commande

```
sudo raspi-config
```

Il faut donc :

— changer le mot de passe
— changer la langue du système
— changer le clavier à mettre en azerty (optionnel car accès en ssh)
— changer le hostname
— mettre à jour le noyau

Le tout se fait dans l'utilitaire ci-dessus. Il ne reste plus qu'à lancer une mise à jour :

Listing 24: Ligne de commande

```
sudo apt update && sudo apt dist-upgrade
```

Borg Toujours en ssh, il est nécessaire d'installer borg sur le Rpi zéro W pour compléter l'installation.

Listing 25: Ligne de commande

```
sudo apt install borgbackup
```

Pour ce qui concerne ce raspberry pi W zéro, l'installation est terminée. Le reste se passera avec la configuration sur le pc avec le lancement de la commande quand ce sera le moment choisi.

4.2 Raspberry pi B (type 3 ou 4)

4.2.1 Installation

Installer et configurer l'installation ne diffèrent pas de son petit frère rpi. Il faut choisir la version de raspberry pi os. Je serais tenté de garder cette version lite mais libre à vous de choisir une version desktop si cela vous sied. Il faut tout de même savoir que ces deux versions desktop ouvrent directement sur le

bureau à l'ouverture avec donc une faille de sécurité qu'il faut pouvoir configurer normalement : mot de passe à l'ouverture.

Il faudra ensuite installer unison pour pouvoir lancer les sauvegardes.

Disque dur Le souhait est d'avoir un NAS le plus petit possible. Il faut donc faire attention à la consommation du disque dur. En effet, sur le raspberry pi, les ports usb sont limités sur ce point là. Il s'agit donc de prendre des disques durs peu consommateurs de courant, soit environ 0.5A et non 1A.

Comme protection, le disque dur sera chiffré. C'est une étape facultative qui peut être oubliée. Il est plus simple de tout faire sur le raspberry pi en ssh.

GNU/Linux possède au niveau de son noyau une solution LUKS pour chiffrer et déchiffrer les dossiers.

La création du volume chiffré va formater le disque dur. Si des données sont présentes, il est important de les copier sur un autre média sans quoi celles-ci disparaîtront. Noter quel est le numéro de la partition de la clé (/dev/sda3) puis démonter le disque.

Ensuite, le disque est à formater et le chiffrement se fera en même temps avec la commande :

Listing 26: Ligne de commande

```
sudo cryptsetup luksFormat -c aes-xts-plain64 -s 512
-h sha512 /dev/sdaXX
```

ou la commande sans sudo sous root. Remplacez XX par le numéro correspondant. Un mot de passe vous sera demandé, il s'agit du mot de passe qui sera demandé à chaque ouverture du disque. Il faut noter que ce mot de passe est à rentrer une fois après le démarrage du micro-pc. Étant donné qu'il restera pour la majeure partie du temps allumé, cette contrainte n'en est pas une.

Puis, il faut créer un système de fichiers :

Listing 27: Ligne de commande

```
sudo cryptsetup luksOpen /dev/sdaXX home
sudo mkfs.ext3 /dev/mapper/home
sudo cryptsetup luksClose home
```

Ainsi, le volume est déchiffré, formater en ext3 puis fermé.

Dans notre cas, deux commandes seront nécessaires pour le monter :

Listing 28: Ligne de commande

```
sudo cryptsetup luksOpen /dev/sdaXX disquedur
sudo mount /dev/mapper/disquedur /home/boum/disque
```

Le disque dur sera déchiffré, puis monté dans l'emplacement du home *disque*.

L'extinction du raspberry pi démontera le disque dur via la commande sur le raspberry pi :

Listing 29: Ligne de commande

```
sudo shutdown now
```

5 La sauvegarde en pratique

La sauvegarde suppose plusieurs types de médias. La figure 1 décrit une architecture possible (la mienne). Il faut noter la présence de plusieurs disques durs.

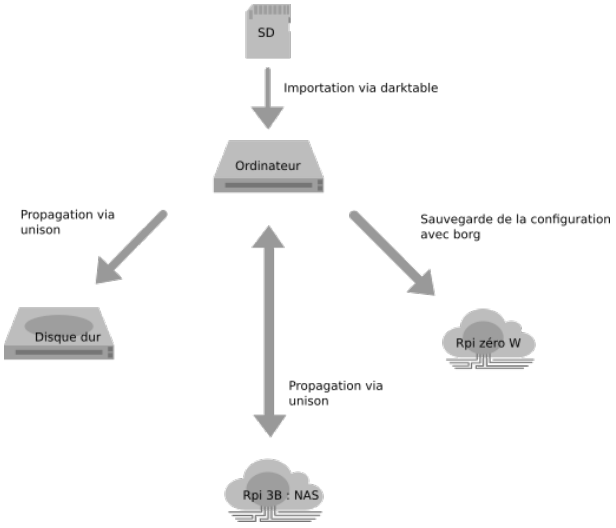

FIGURE 1: Architecture de la sauvegarde : exemple

Pour l'instant, la façon de faire peut être compliquée étant donné l'unique poste de travail. Cependant, elle sera prête si une évolution est faite vers du multi-postes.

Conclusion

Ce tutoriel se conclut par un exemple d'architecture. Étant donné qu'il existe une multitude d'installations, je ne présente pas la façon pratique de mettre cela en place. Si d'aventure, cela intéresse, mon mail est disponible et cela pourra faire l'objet d'un billet sur le blog.

Il est vrai que cela demande du temps, mais lorsque celle-ci est finie, il est assez gratifiant de retrouver toutes les données si il y a un bug.

Cela n'arrive pas qu'aux autres.

6 Bonus : sauvegarder en voyage

6.1 Type de disque dur

Le voyage est quelque chose qui bouge, il est nécessaire d'avoir des outils qui tiennent la route et qui ne cassent pas au moindre choc.

Si nous reprenons, il existe deux grands types de supports :

— le disque dur mécanique

— le disque ssd

Chacun a ses avantages et ses inconvénients. Voyons quelques points :

Caractéristiques	Disque dur mécanique	Disque dur ssd
Résistance aux chocs	-	++
Prix	+	++
Capacité	+	-
Rapidité en usb	-	+

Ces données dessinent un peu mieux le panorama des endroits où devraient être utilisés les disques de chaque type. Il est cependant difficile, la majeure partie du temps, de concilier la donnée du prix et celle de la capacité.

6.2 Ordinateur en voyage

6.2.1 Introduction

En voyage, il n'est pas forcement nécessaire d'avoir un ordinateur portable. D'une part, cela prend de la place et donc du poids. Et d'autre part, le développement n'est pas quelque chose qui se fait sur ce type de machine, l'écran n'étant pas ce qu'il y a de mieux pour développer. Enfin, le développement n'est peut-être pas à faire pendant le voyage. Il peut attendre d'être fait à tête reposée.

La réflexion a été d'utiliser un raspberry pi que j'avais déjà et son large écosystème. Le projet avec alimentation, lecteur carte sd, disque ssd et câble sata/usb pèse 292g ; soit un poids assez contenu. Par rapport à un portable basique qui approche ou dépasse le kilogramme, il y a un gain de poids à considérer.

Il est vrai qu'il existe déjà en vente des systèmes autonomes, mais le prix n'est pas exactement le même. On passe à 171 € contre moitié moins pour ce système, mais cela dépend surtout du type et de la taille du disque dur que l'on ajoute.

On peut aussi parler du smartphone avec l'otg mais la place ensuite n'est pas si extensible que cela, il me semble qu'il vaut mieux dans ce cas acheter des cartes SD plutôt que des micro-sd.

L'inconvénient reste l'absence de courant, mais une batterie externe peut être utilisée. Il faut aussi voir les accès possibles à l'électricité qui sont largement courants.

6.2.2 Matériel

La liste minimum comporte 4 items :

— un raspberry pi 3 : même le 4 à la rédaction du tutoriel, 39 €. Cette version a aussi l'atout d'avoir plus de pêche au niveau électrique et des ports usb3.
— son alimentation usb C : 9 €
— une carte micro-sd pour le système : 10 € pour une 16 Go (probablement même moins)
— l'écran tactile pour raspberry pi, celui commandé a été envoyé avec un boîtier, en direct de banggood.com : 13 € à l'époque par exemple : ici

Le système de base revient à environ 70 €. Il suffit ensuite d'ajouter un moyen de lire la carte sd ou relier simplement l'appareil photo au raspberry pi et un disque dur externe que ce soit mécanique mais fragile ou ssd mais plus cher.

6.2.3 Préparation du raspberry pi

Carte sd Les étapes sont :

- Télécharger la dernière version de raspberry pi OS : version desktop sans les programmes recommandés. j'ai d'ailleurs encore désinstallé des choses après installation (libre-office et éditeurs de codes) à vous de choisir sur cette page
- Décompresser le zip
- Lancer l'installation sur la carte sd sous bash avec dd :

Listing 30: Ligne de commande

```
sudo dd bs=4M if=fichier.img of=/dev/sdb conv=fsync
```

Attention à bien sélectionner le fichier source mais surtout le périphérique de sortie et ceci afin de ne pas effacer le disque du système. La ligne précédente n'est qu'un exemple, c'est à adapter à votre configuration !

- activer l'accès à distance ssh en créant un fichier nommé ssh dans le volume boot ; dans le bon répertoire un *touch ssh* fait l'affaire, le fichier peut être vide
- activer le wifi avec un fichier wpa.supplicant.conf sur le volume boot contenant

Listing 31: wpa.supplicant.conf

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
country=FR

network={
  ssid="SSID"
  psk="PASSWORD"
  key_mgmt=WPA-PSK
  scan_ssid=1
}
```

Changer les termes entre guillemets en les laissant par les bons paramètres de votre installation.

La carte sd est maintenant prête.

Premier démarrage Mettre le rpi sous tension avec la carte SD branchée. Laisser du temps avant de vous brancher en ssh.

Listing 32: Ligne de commande

```
ssh pi@raspberrypi
```

Le mot de passe est raspberry

Il est nécessaire de changer des paramètres pour sécuriser le micro-pc avec l'utilitaire raspi-config

Listing 33: Ligne de commande

```
sudo raspi-config
```

Il faut donc :
— changer le mot de passe
— changer la langue du système
— changer le clavier à mettre en azerty
— changer le hostname
— mettre à jour le noyau

Le tout se fait dans l'utilitaire ci-dessus. Il ne reste plus qu'à lancer une mise à jour :

Listing 34: Ligne de commande

```
sudo apt update && sudo apt dist-upgrade
```

Et redémarrage

Listing 35: Ligne de commande

```
sudo reboot
```

6.2.4 Écran tactile LCD

Installation Toujours sur le raspberry, il s'agit tout d'abord d'installer git :

Listing 36: Ligne de commande

```
sudo apt install git
```

Puis d'installer et de lancer le driver de l'écran tactile :

Listing 37: Ligne de commande

```
git clone https://github.com/waveshare/LCD-show.git
cd LCD-show/
chmod +x LCD35-show
./LCD35-show
```

Pour les deux dernières commandes, il est nécessaire que l'écran acheté correspond à ce driver (XPT2046) avec la taille de l'écran à 3,5".

A la suite de ces commandes, le raspberry va redémarrer et l'écran marchera. Attention, si vous aviez branché un écran HDMI, celui-ci n'aura plus d'image.

Calibration de l'écran C'est l'étape la plus délicate, il a fallu que je tâtonne quand à cette partie. A mon sens, cette partie est plus facile lorsque les commandes hors calibration se font via ssh. J'ai branché juste un clavier pour parvenir au programme "calibrator" installé via :

Listing 38: Ligne de commande

```
sudo apt install xinput-calibrator
```

Le fichier de configuration /usr/share/X11/xorg.conf.d/99-calibration.conf est à modifier en premier en changeant la variable de SwapAxes à 0 au lieu de 1. Ce fichier est à modifier en root :

Listing 39: Ligne de commande

```
sudo nano /usr/share/X11/xorg.conf.d/99-calibration.conf
```

Redémarrer le PC et lancer le programme de calibration situé dans le menu/-préférences. Cliquer avec un stylet sur les croix qui apparaissent. A la fin de cette étape, il y aura une suite de chiffres à changer dans le fichier de configuration . Enfin, l'étape de redémarrage est à refaire.

Si d'aventure, l'écran est mal orienté , le script d'installation est à exécuter de nouveau avec l'argument en degrés pour faire tourner l'écran soit 90, 180 ou 270. Par exemple :

Listing 40: Ligne de commande

```
./LCD35-show 180
```

Il sera nécessaire ensuite de reprendre toute la calibration avec les étapes décrites ci-dessus, en résumé :

- lancer le script : ./LCD35-show avec les arguments voulus
- mettre la variable SwapAxes à 0 dans le fichier de configuration : /usr/share/X11/xorg.conf.d/99-calibration.conf
- calibrer l'écran avec calibrator dans le menu préférences
- enregistrer les nombres données dans le fichier de configuration (le même)

6.2.5 Conclusion

Pour le prix, cela donne un résultat satisfaisant. De plus, si un accès a une prise HDMI, il est toujours possible de se brancher. Avec les périphériques d'entrée, ce petit objet deviendra un véritable pc tel que la majeure partie des gens l'entend (c'est déjà un pc à la base). Il faudra simplement réactiver la sortie hdmi via la commande :

Listing 41: Ligne de commande

```
./LCD-hdmi
```

Il sera nécessaire ensuite de relancer la commande adéquate pour réactiver l'écran :

Listing 42: Ligne de commande

```
./LCD35-show
```

Il ne reste qu'à configurer des raccourcis sur l'écran qui enregistrent automatiquement les clichés de la carte sd au disque dur ou pour autre besoin.