# Installation de replicant: prérequis et explications:

Tout d'abord, sur le fonctionnement de ce document.

Les liens en bleu renvoient vers des sites internet quand on clique dessus.
Les liens en bleu clair renvoient vers d'autres pages et endroits de ce pdf.

Les commandes à faire dans un terminal sont avec une autre écriture et aussi en bleu, et donc renvoient vers des sites qui expliquent ces commandes. Exemple:
`ls -actrl`
Pour ce tutoriel il n'y a pas besoin de comprendre entièrement ces commandes, vous pouvez les copier-coller. Mais il y a les liens pour que vous puissiez approfondir.

Pour pouvoir installer replicant, le mieux est d'avoir un ordinateur avec GNU/Linux installé dessus, ou alors n'importe quel ordinateur qui démarre avec une clé usb de démarrage GNU/linux.

Sur cet ordinateur, les programmes nécessaires sont:
- heimdall: souvent on peut l'installer avec les gestionnaires d'installation classiques
- gpg
- gparted ou équivalent
- adb pour la sauvegarde (optionnel)

L'idée de ce tutoriel est de montrer une manière d'installer replicant qui utilise la carte microSD, et d'éviter de parler de toutes les possibilités dans le but de simplifier.

Sommaire:

# Installation de replicant sur un Samsung S3 i9300

Tutoriel pas-à-pas, pour l'installation de base. Le but est de montrer simplement toutes les étapes.
Alors pourquoi replicant?


Parce qu'il s'agit d'un système 100% libre. Il est dérivé d'Android et maintenant de LineageOS, et permet d'éviter d'utiliser des programmes propriétaires.

Pour un téléphone qui est potentiellement soumis à plus d'attaques (parce que potentiellement on l'emmène avec nous et donc ça nous "suit") la sécurité et le 100% logiciel libre sont importants.

Pourquoi ce modèle de téléphone et pas un autre? Il y a aussi le **Galaxy Note 2 (N7100)**, et le **Galaxy Note 8.0 (N51xx)** qui sortent du lot en termes de compatibilité.

Mais le Galaxy S3 i9300 est celui sur lequel les gens de replicant, qui ont très peu de moyens, travaillent le plus. Pour la prochaine version de replicant, replicant 9, ce sera d'abord ce modèle qui tournera dessus.

Je viens de voir très récemment qu'il y a un autre projet de téléphone libre ( https://www.pine64.org/pinephone/ )

Pourquoi un smartphone?

Cela permet d'avoir accès à des programmes spécifiques qu'on ne trouve pas forcément sur les ordinateurs, d'avoir quelque chose de miniaturisé comme un ordinateur et encore plus petit, de ne pas laisser ce terrain au capitalisme de surveillance, et d'avoir un téléphone plus sûr.

**D'abord tout sauvegarder, si vous avez des documents.**
Un grosse microSD de 32Go doit faire l'affaire, ou alors une clé usb, un disque dur externe avec un adaptateur usb OTG, … c'est pas toujours évident! Surtout pour sauvegarder certaines choses comme les sms.

Si on part d'un téléphone d'occasion venant de quelqu'un d'autre, on ne se pose pas ces questions.

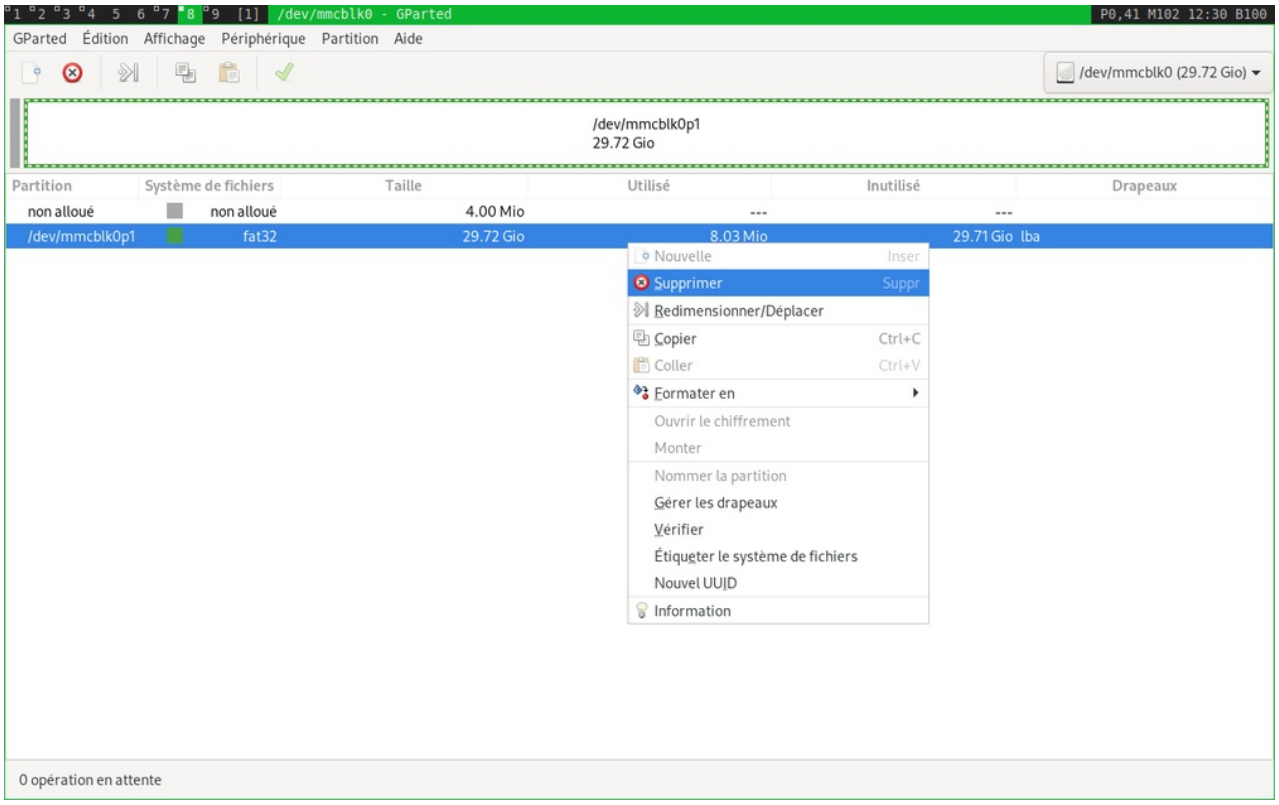
On va commencer par formater la carte microSD dont on aura besoin plus tard. Donc la mettre dans un adaptateur SD - microSD et dans un ordinateur qui a la prise SD qui va bien. (sinon il y a aussi des adaptateurs microSD USB, mais tous ne marchent pas).

Dans le navigateur de fichiers, s'arranger pour la démonter, comme montré page 22 (cliquez ici pour aller page 22).

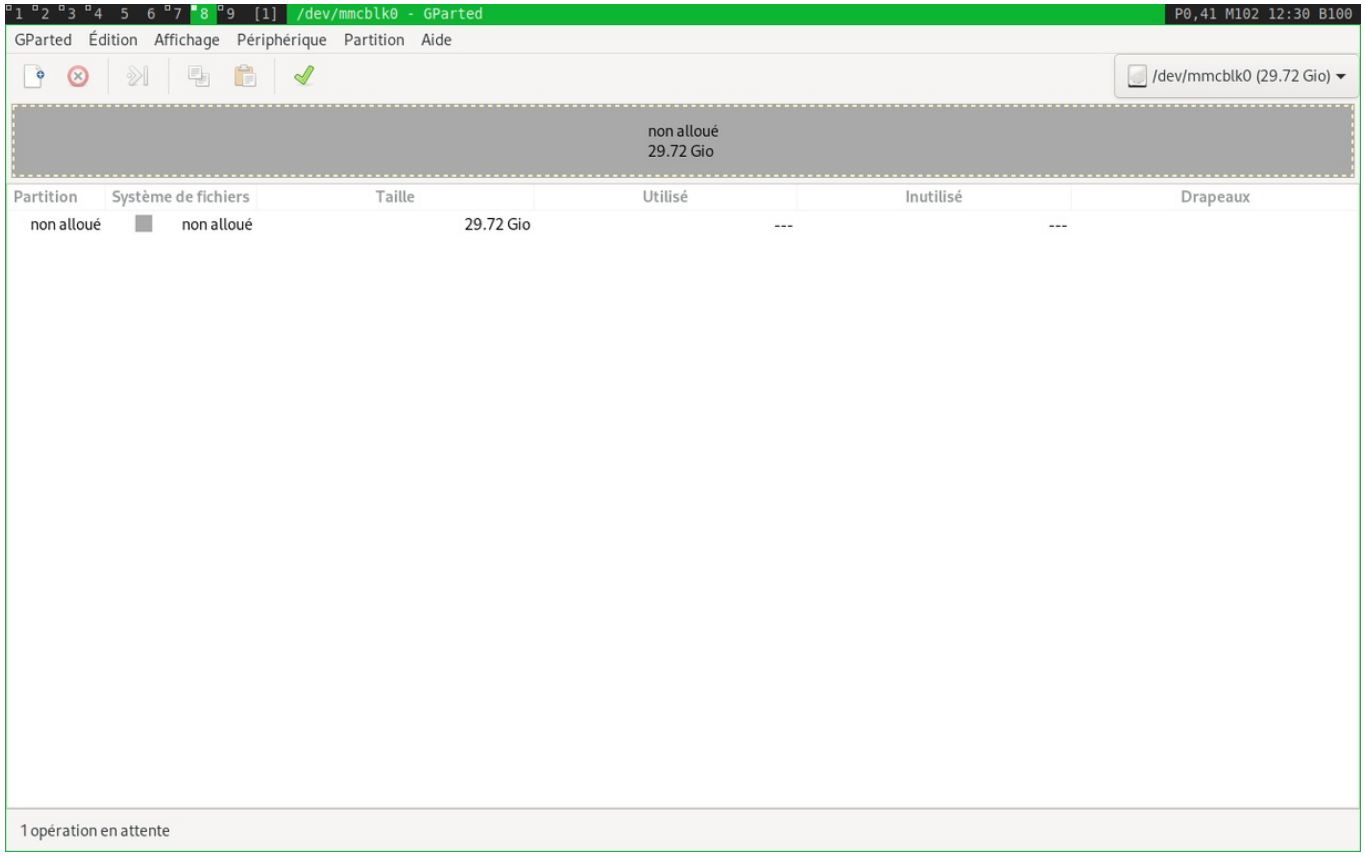
On va la reformater. Je le fais avec gparted, qu'on trouve en général sur un système GNU/linux.

**Faire très attention de bien être sur la bonne partition, surtout pas sur le disque dur de l'ordinateur!! /dev/mmcblk0 et la taille en Go donnent une indication.**

La commande
`lsblk`
dans un terminal fait aussi un bon bilan de ce qui est branché comme support de mémoire.

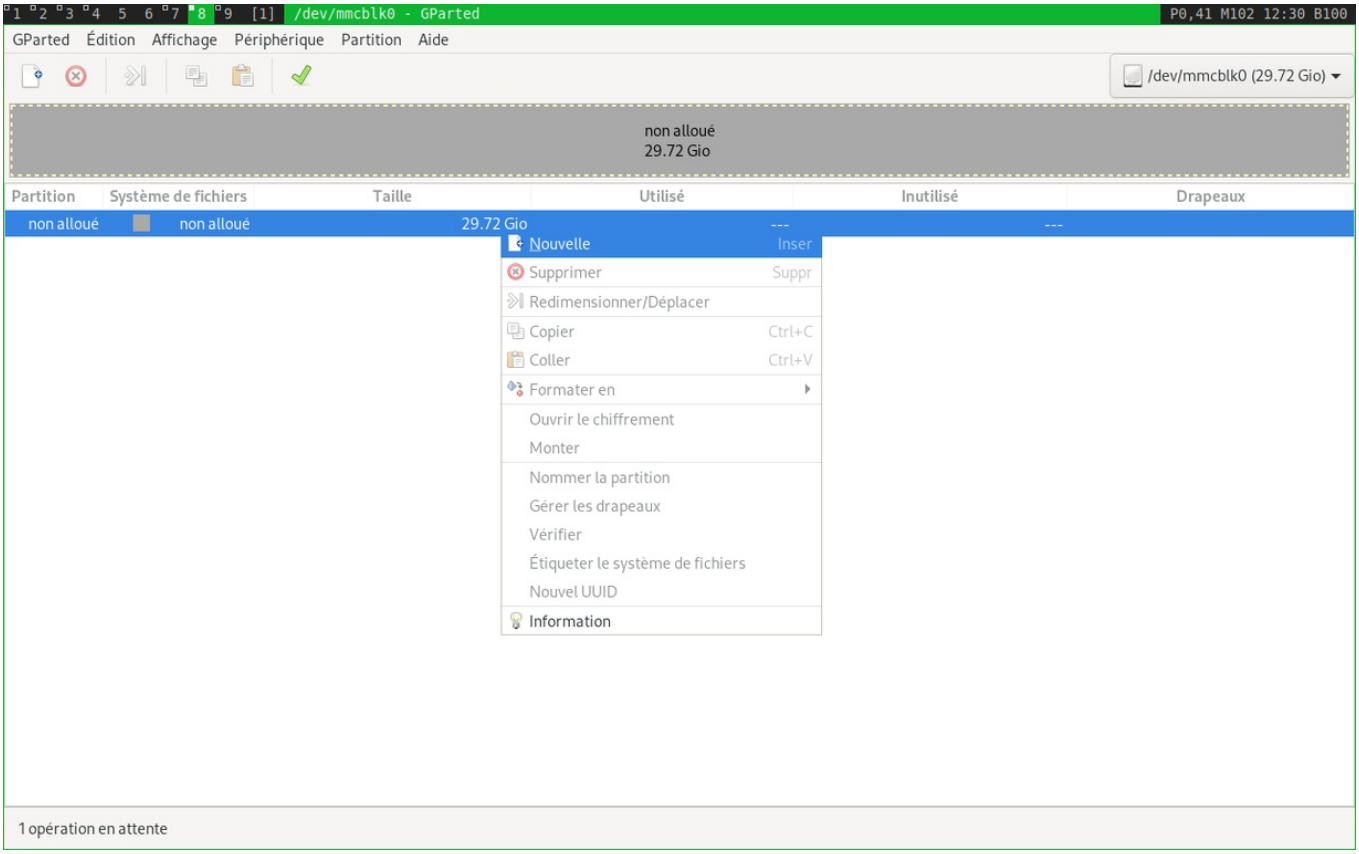



Dans gparted on fait clic droit supprimer, pour supprimer la partition existante du fabricant. On pourra aussi récupérer les 4Mo non alloués.

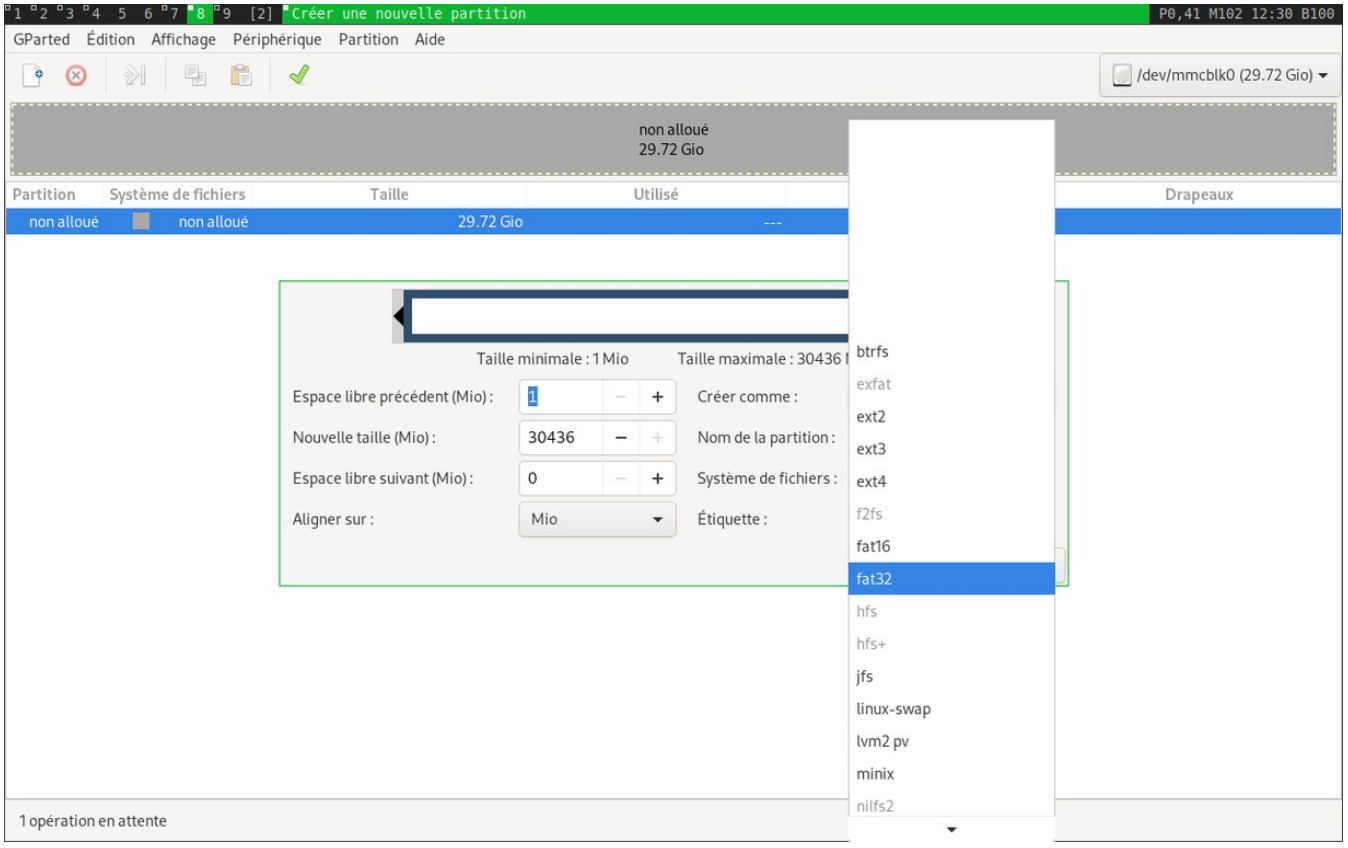


Voici le résultat.

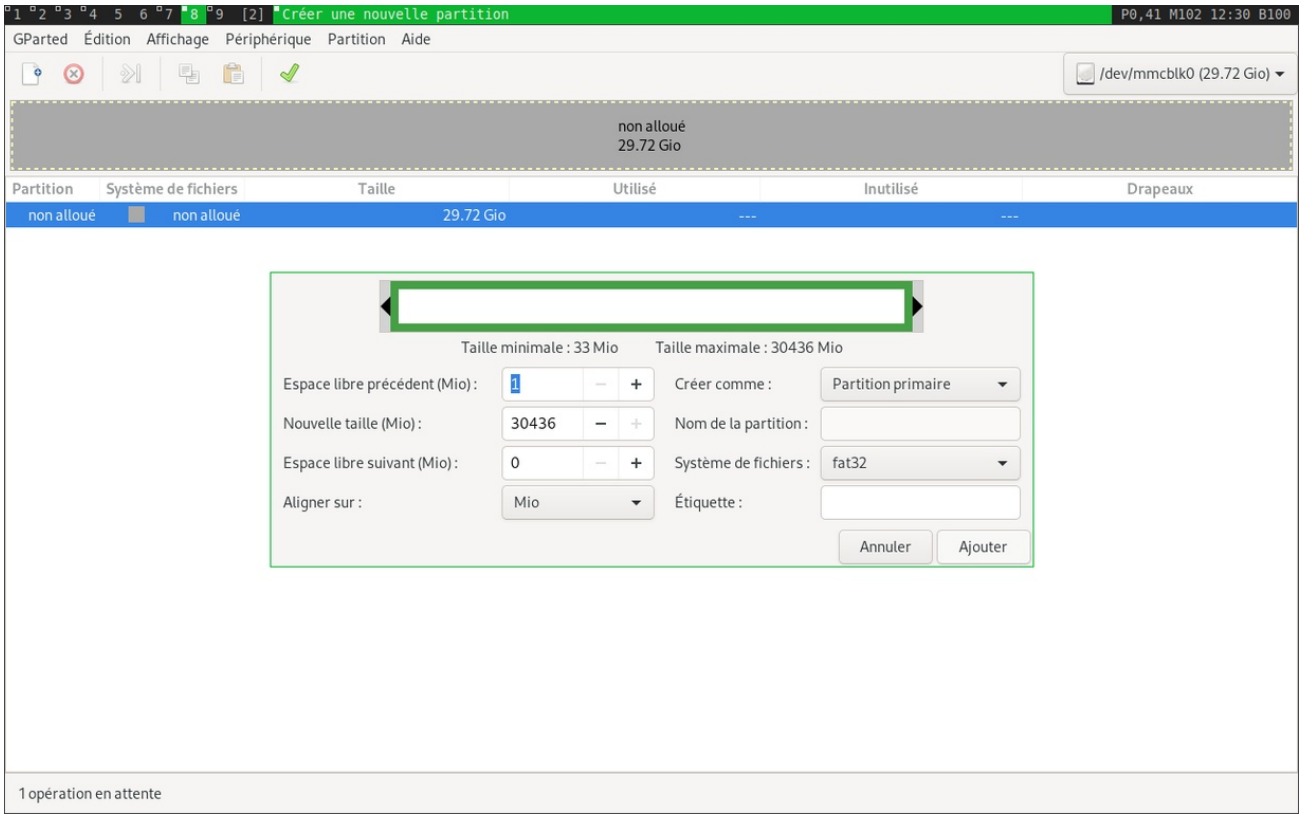
Puis on fait clic droit, puis "nouvelle".



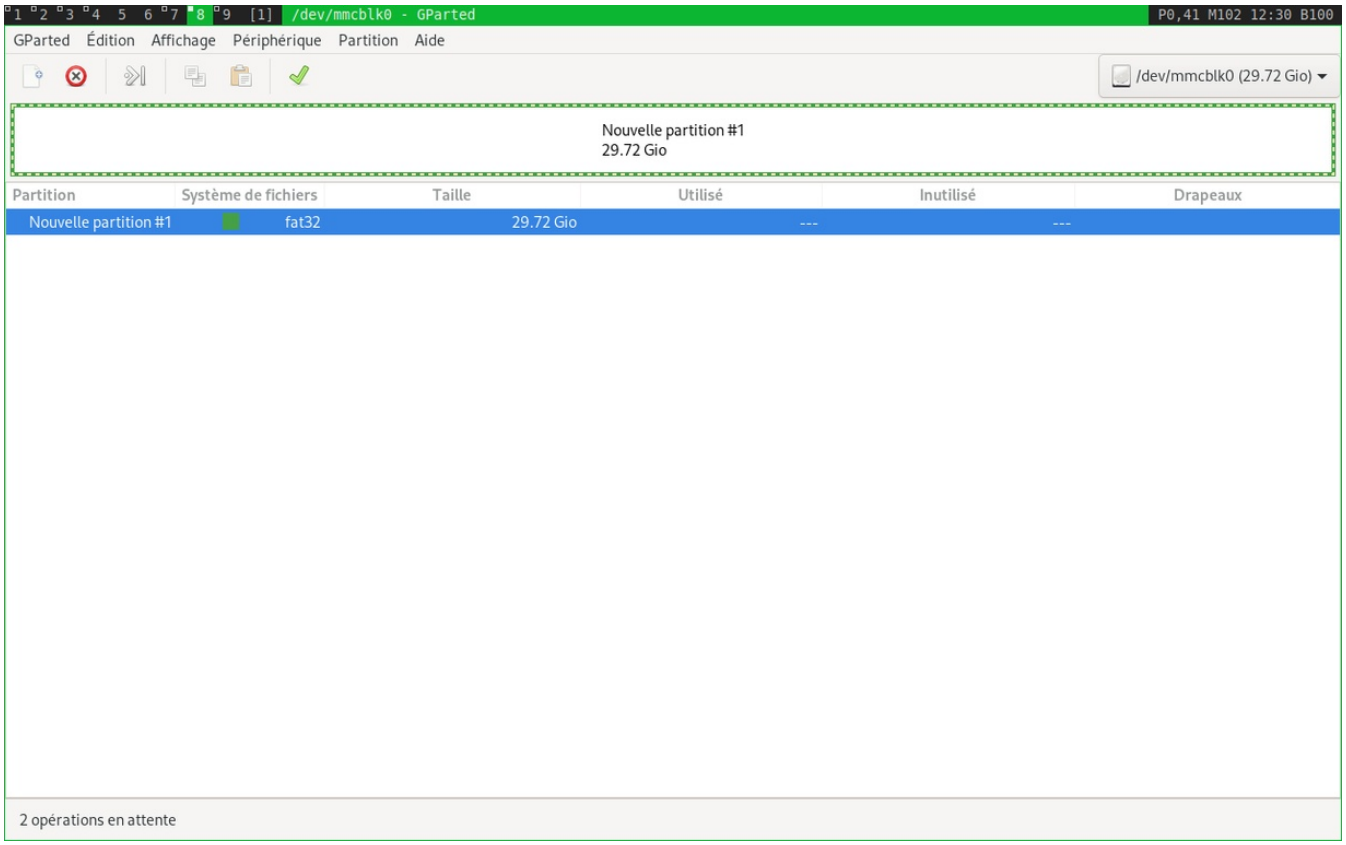

Dans systèmes de fichiers, on choisit "fat32"



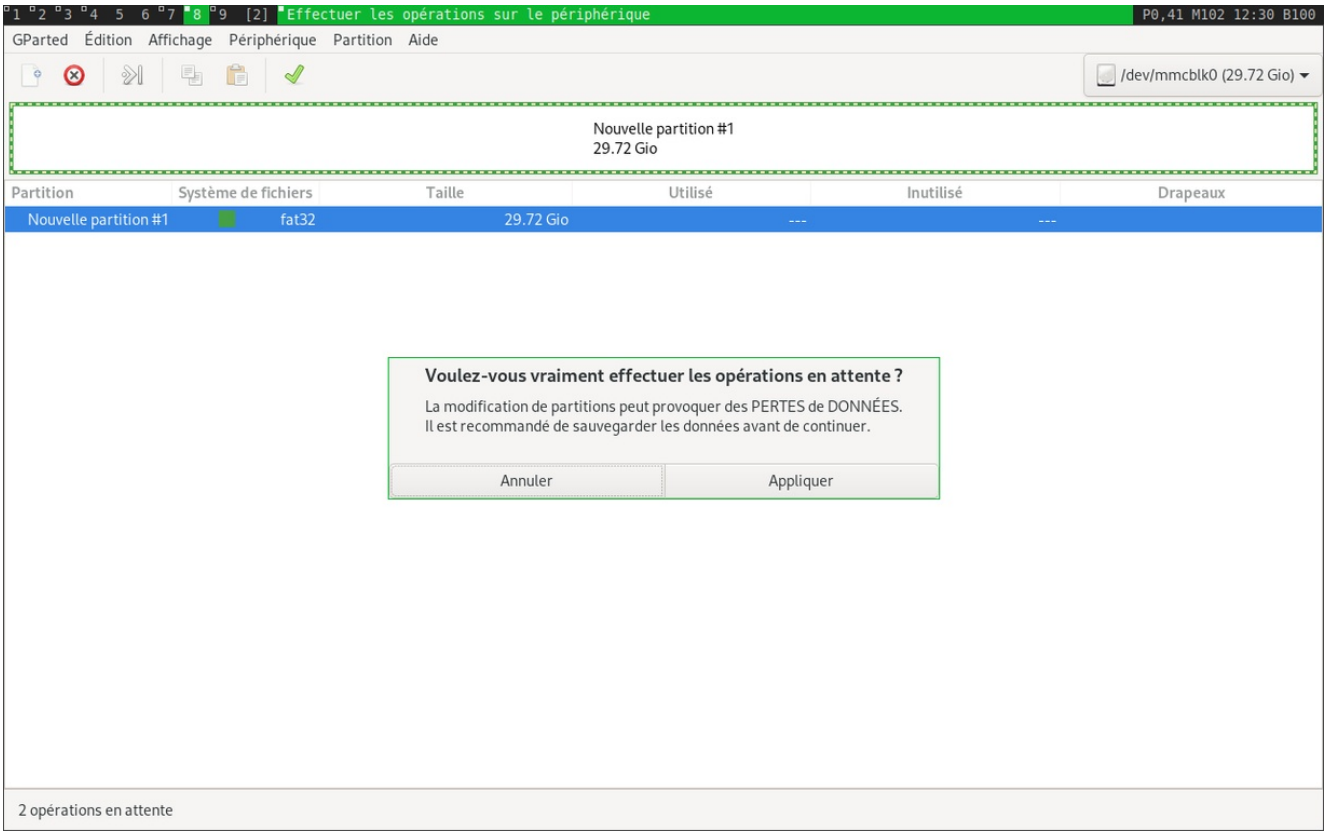

C'est ce qu'il y a de plus courant pour une clé usb.



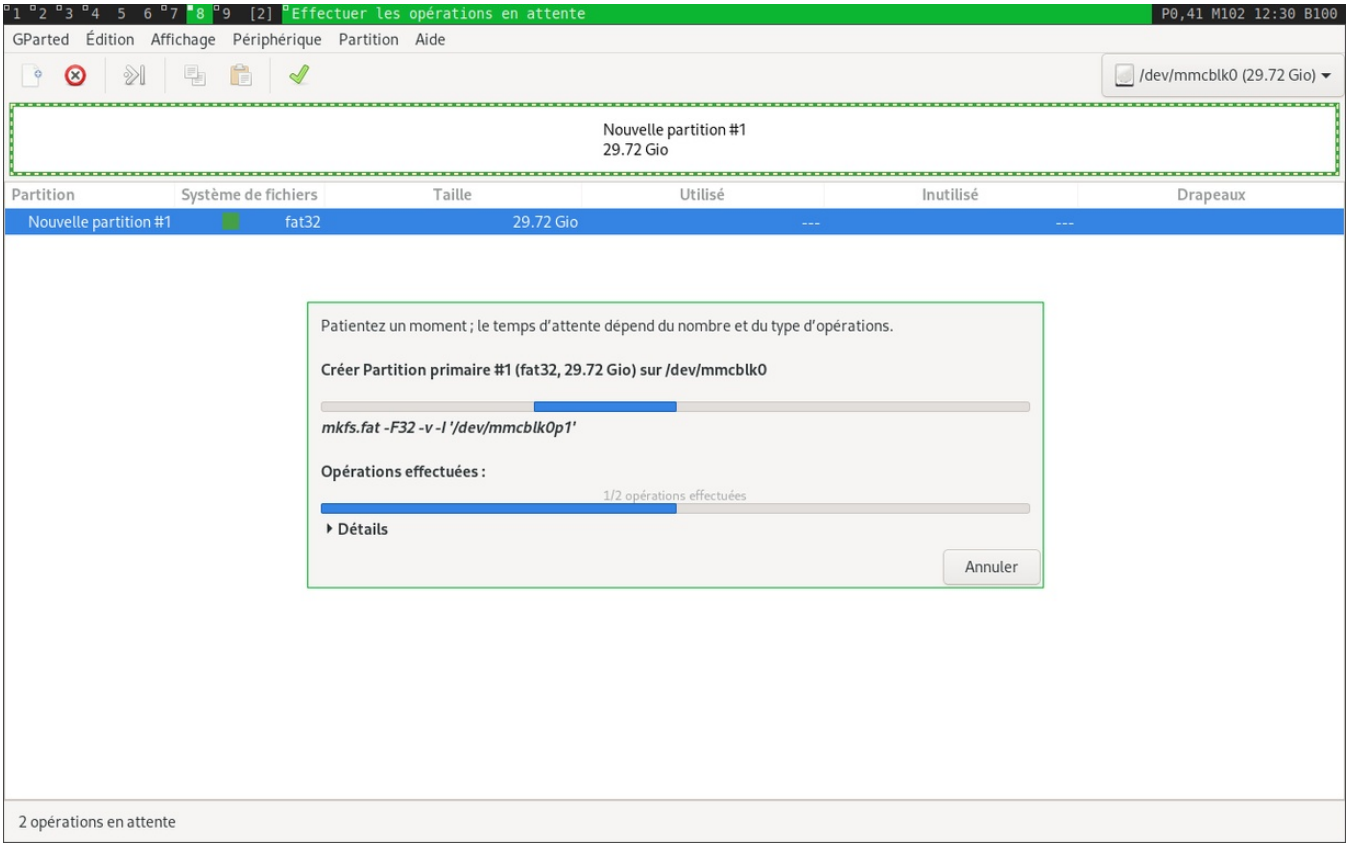

Voici le résultat. Les flèches à côté du rectangle vert servent à redimensionner. Là on en aura pas besoin.



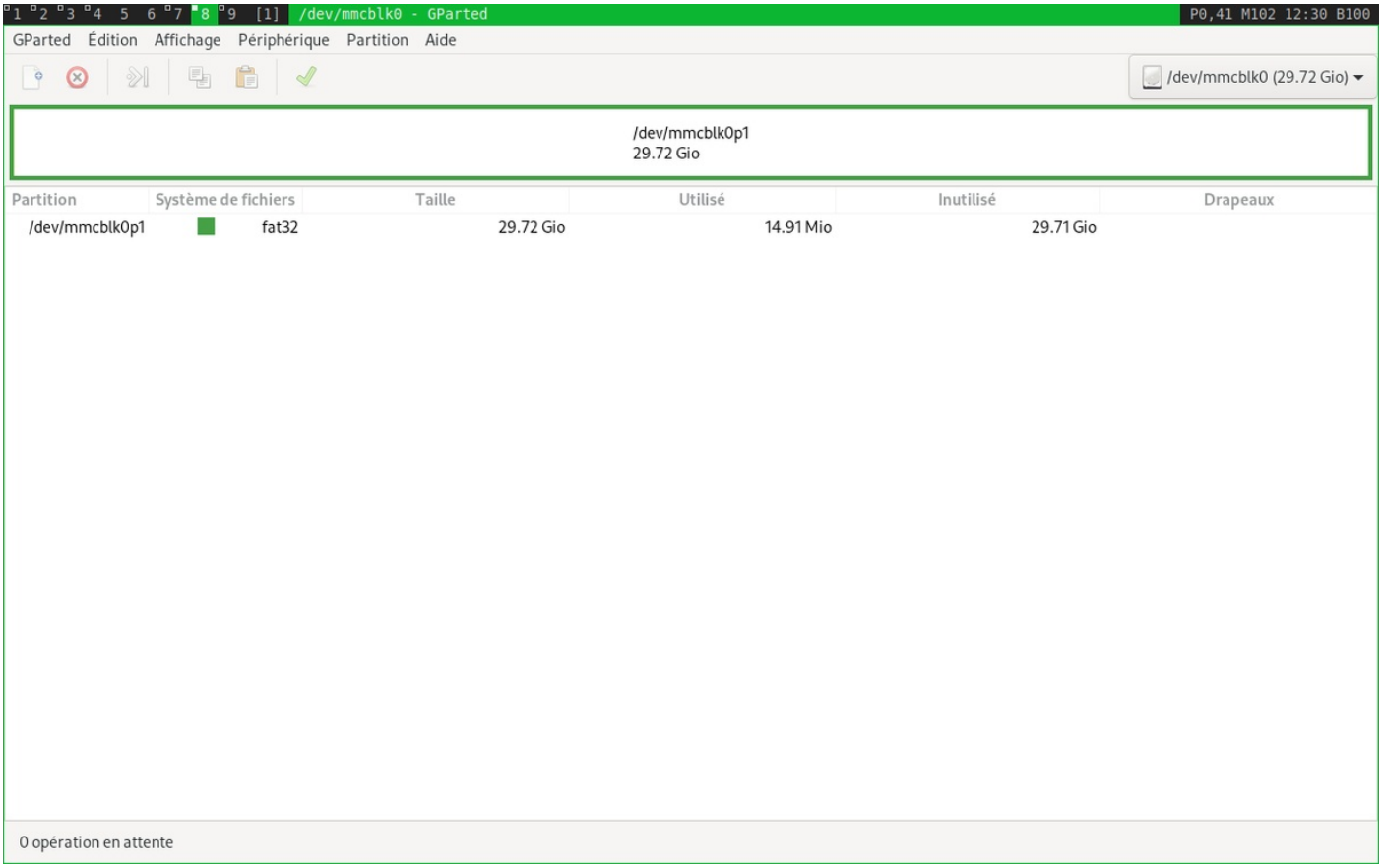

Résultat. À ce stade si on annule tout, la microSD est encore indemne et non modifiée. Mais on est sûr de ce qu'on veut faire, et on écrit pas sur le disque dur.




Donc on clique sur le V vert, et on nous demande si on est vraiment sûr. Faire "Appliquer".

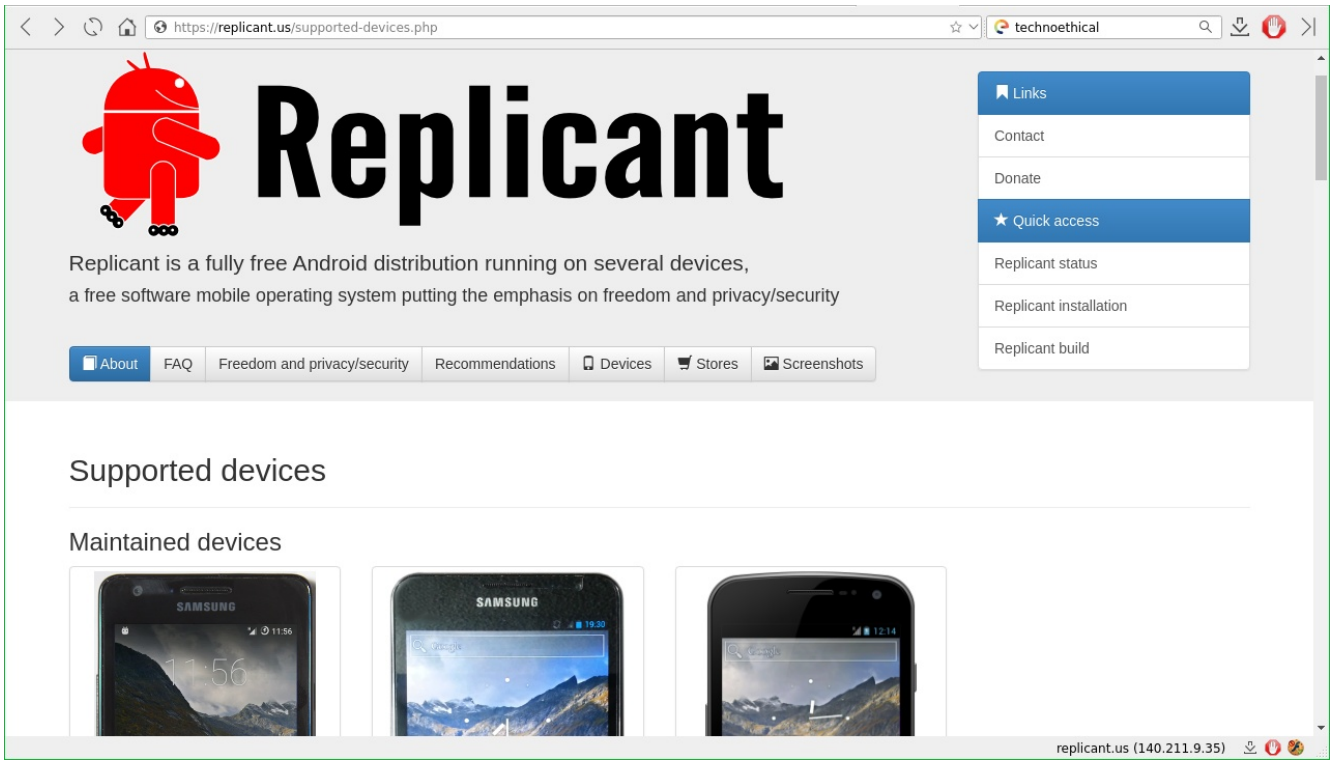



Voilà ce qu'il fait comme commande pour formater.  J'ai pas eu le temps de cliquer sur "Détails".

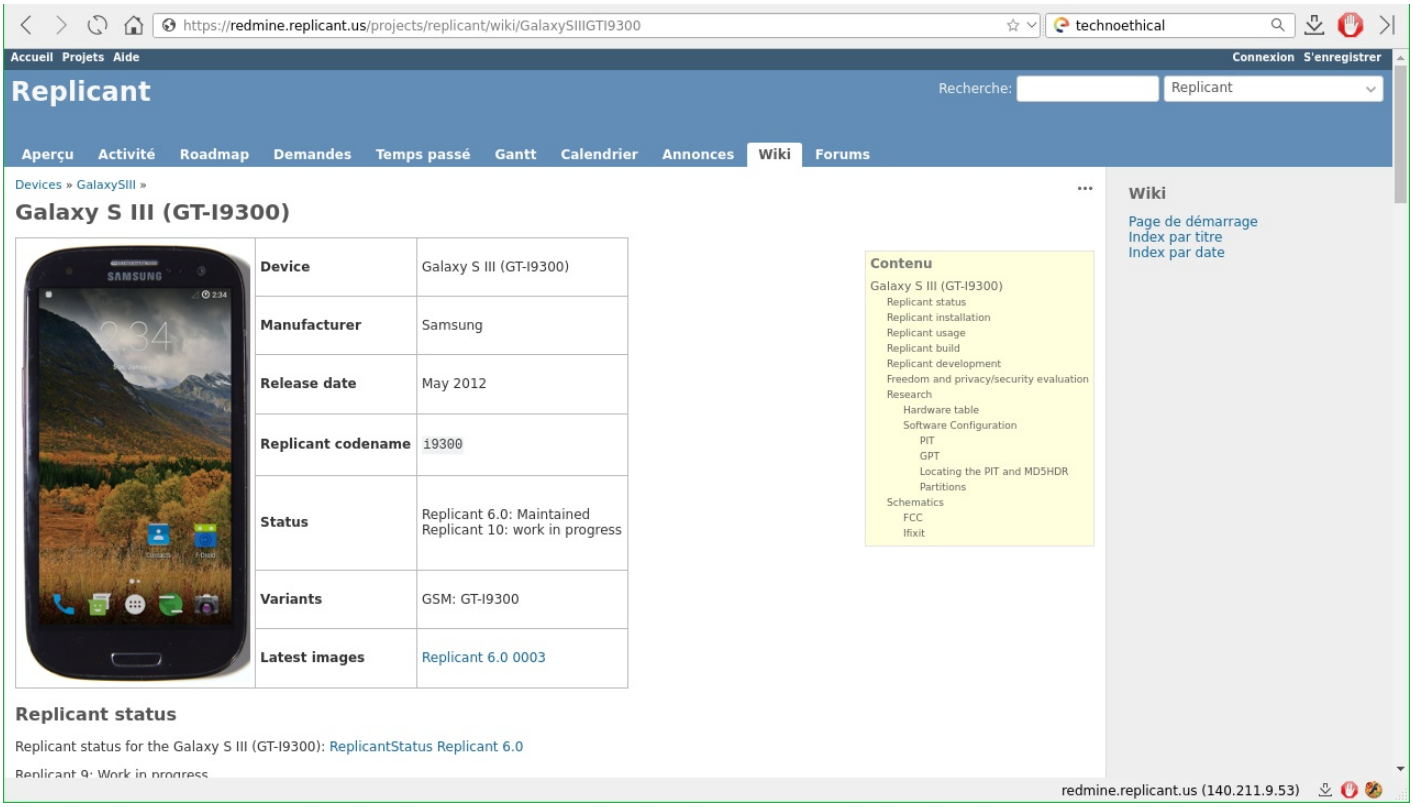



Et voici le résultat, et notre carte microSD formatée!

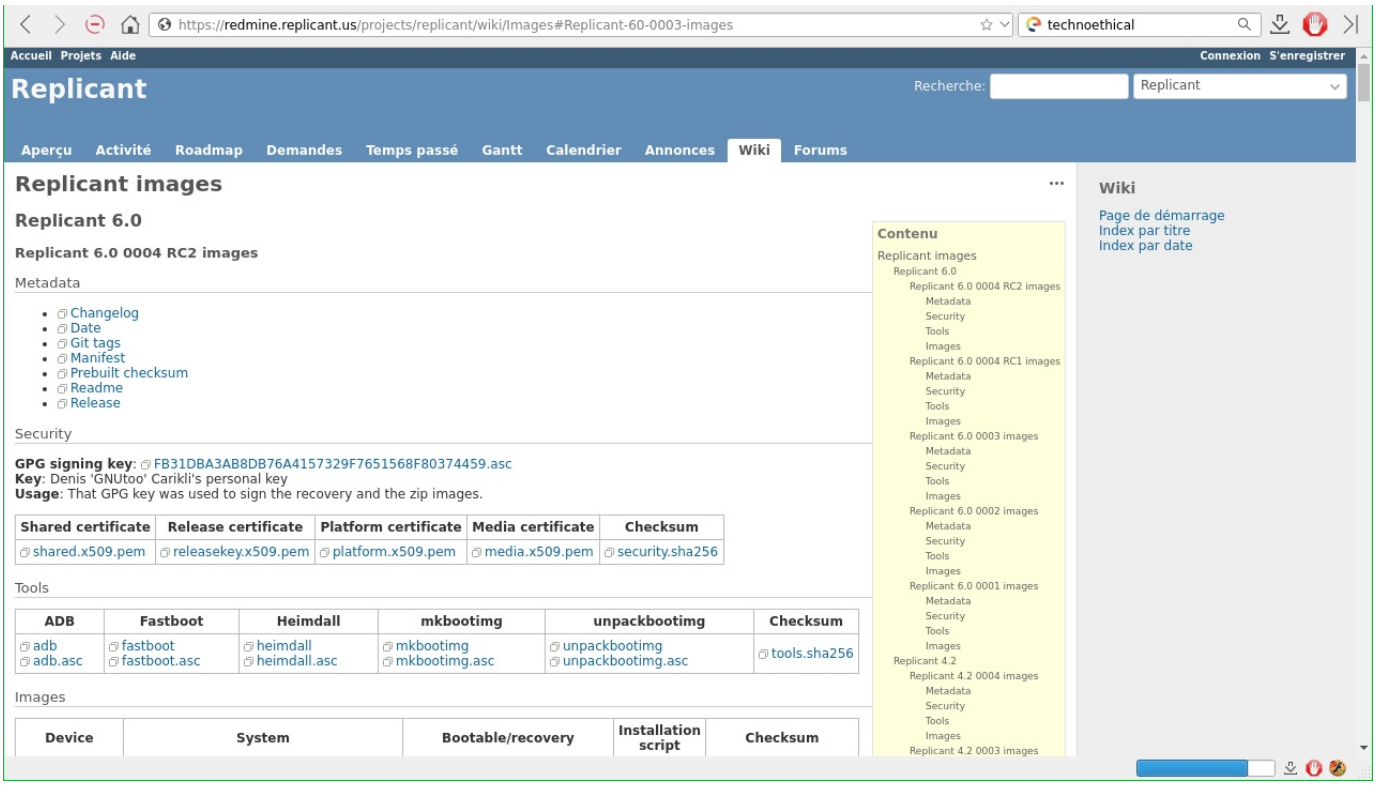
Maintenant on va télécharger le système replicant de manière sécurisée, et le mettre sur une carte microSD.




On clique sur l'onglet "devices" sur le site https://replicant.us
On arrive à la liste des modèles où on peut installer replicant.
On clique sur le galaxy S3 i9300.



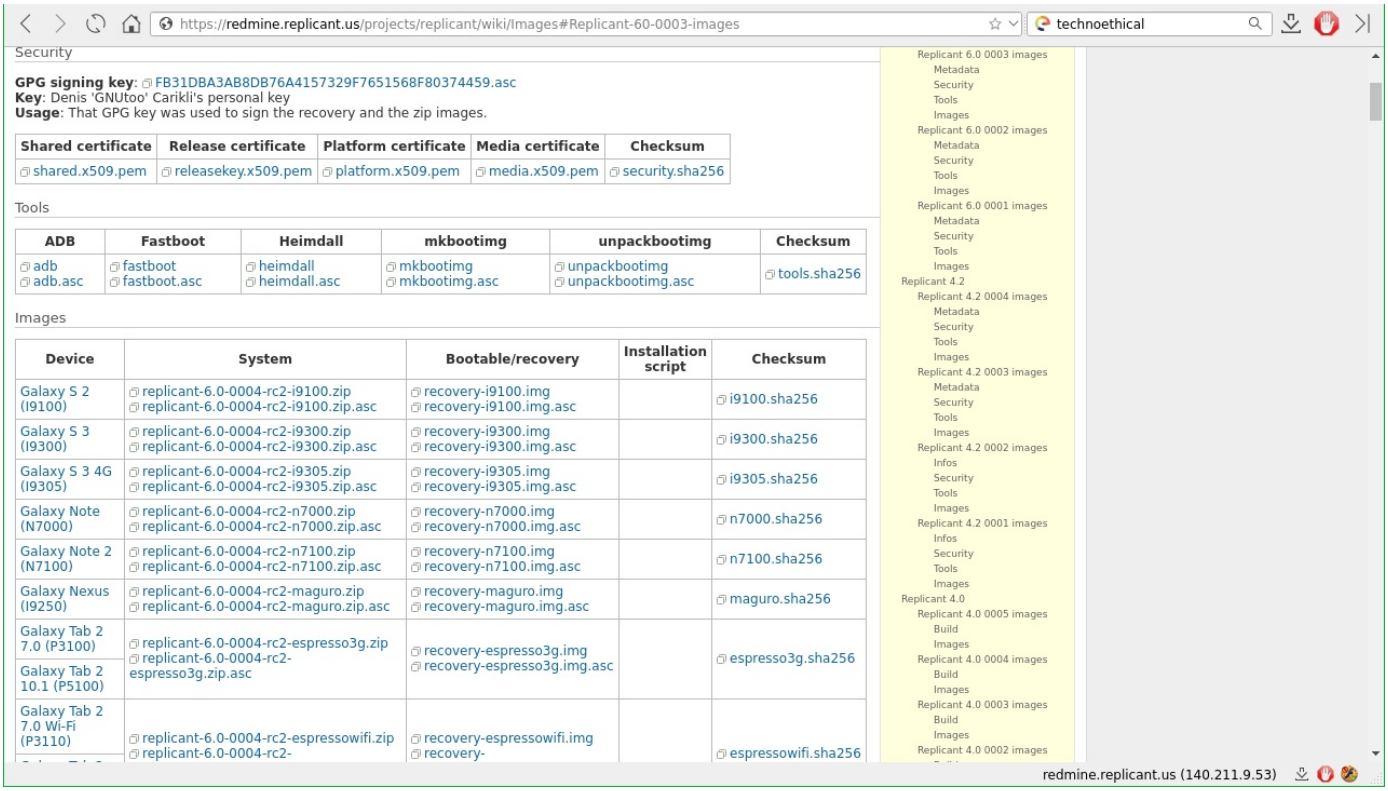

On clique sur "Replicant 6.0.003" qui est la dernière version stable conseillée.
Attention dans ma démo j'ai pris la version 004. Les versions changent régulièrement.
**Installer la 003, qui est propre et sans bugs. Le reste est pareil, sinon.**



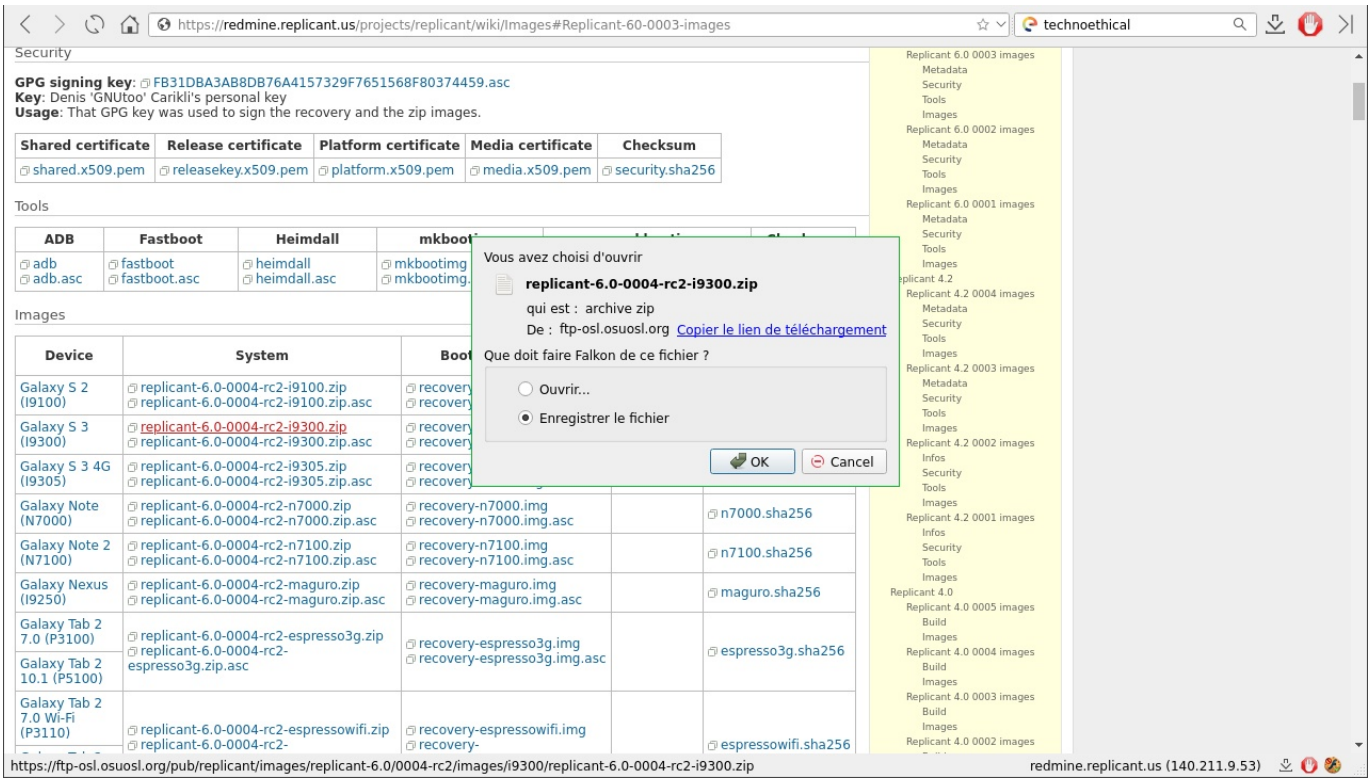

On va télécharger un certain nombre d'informations de cette page.
Un certain nombre de choses sont faites pour s'assurer qu'on télécharge bien ce qui vient de ce site et pas autre chose.
Pour éviter que quelqu'un qui se fait passer pour le site introduise sa propre version du système; ce qui peut être une attaque informatique.
Il va être pratique de créer un répertoire replicant pour mettre tout ce qu'on va télécharger:

```
mkdir ~/replicant
```

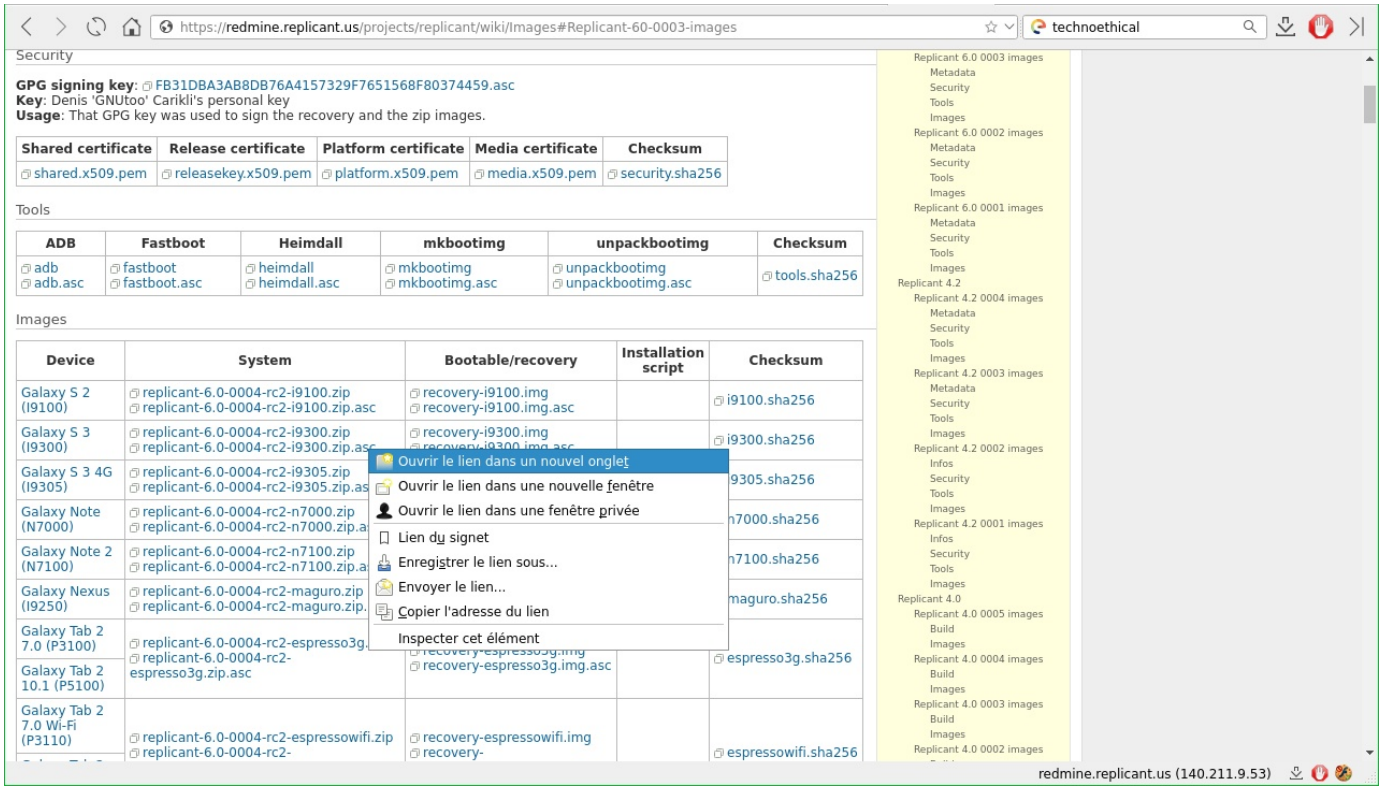
Est une commande faite dans un terminal (xterm, lxterminal, autre, voir plus loin) qui permet de créer un dossier replicant dans son espace utilisateur, le chemin sera /home/user/replicant



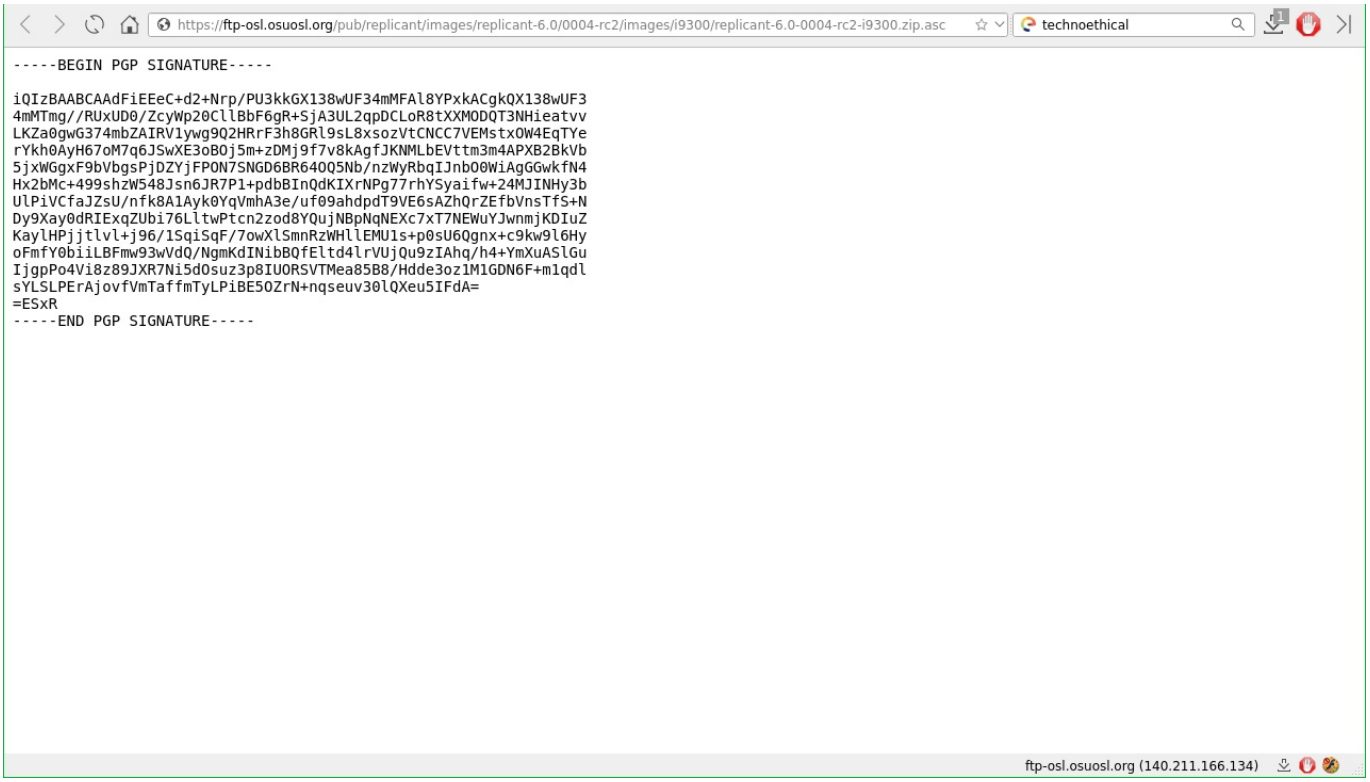

Ici on a la liste des modèles avec la dernière version du système et les différents systèmes de chiffrement et signatures. Il faut faire attention à télécharger uniquement ce qui concerne le modèle i9300! Et pensez bien à choisir la 003.




On télécharge le système replicant replicant-6.0-004-rc2-i9300.zip.
Le .zip est un format d'archive qui permet de regrouper et compresser des fichiers.
On enregistre le fichier.

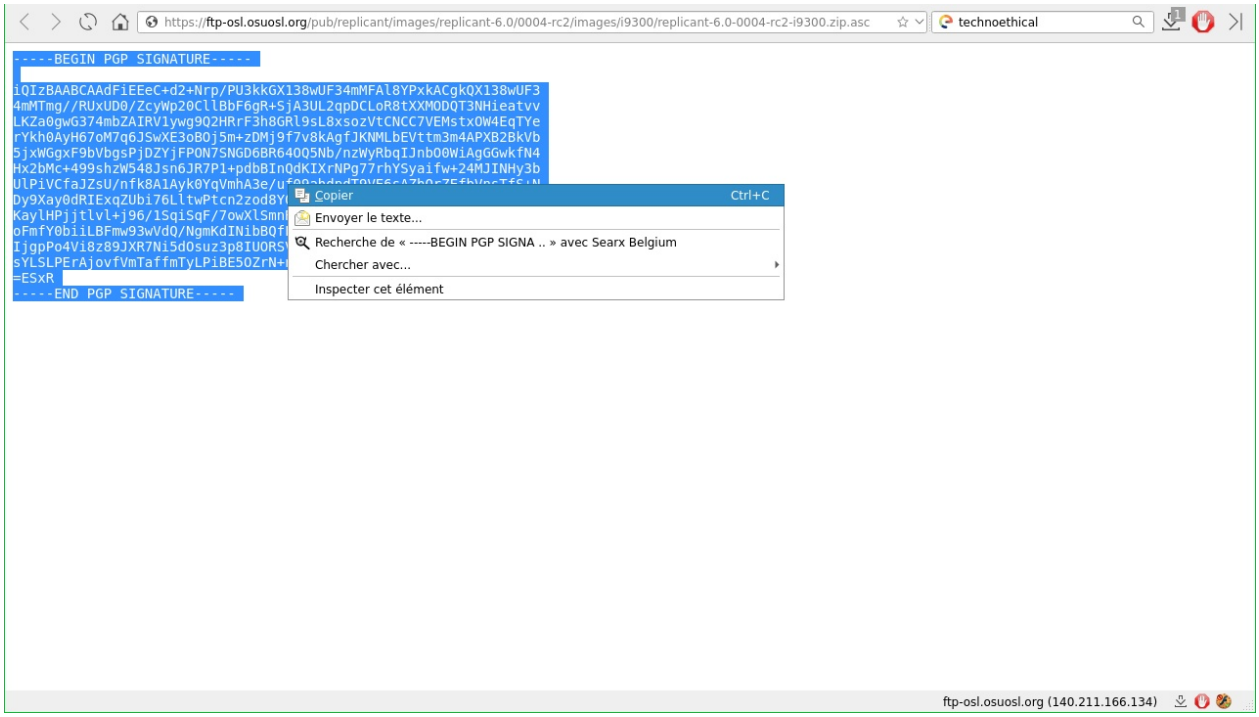



On fait clic droit puis "ouvrir dans un nouvel onglet" pour le fichier .asc qui correspond à l'archive .zip qu'on a téléchargé juste avant.

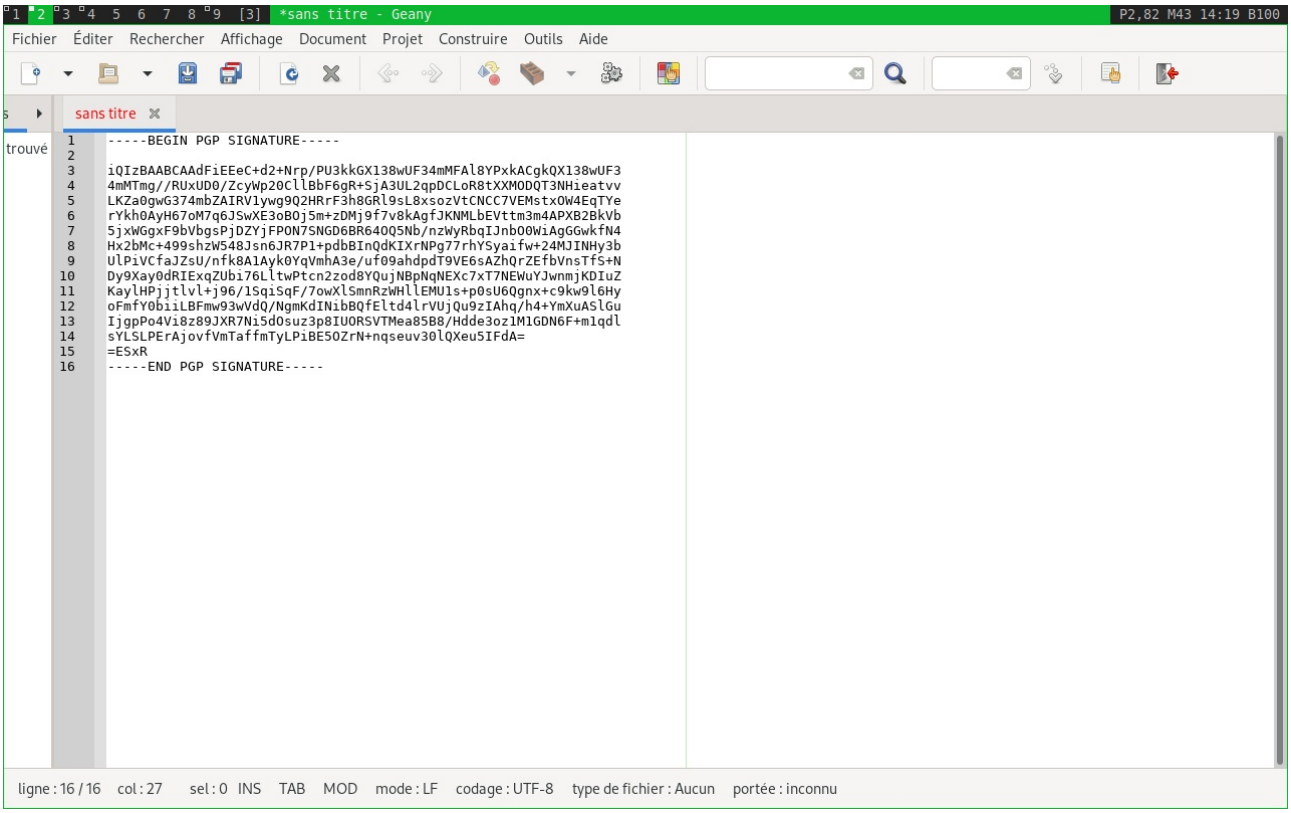



Le nouvel onglet ressemble à cela.
C'est une signature pgp.
Cela permet de savoir si le fichier .zip correspond bien à la bonne personne.

gpg est un système de chiffrement très utilisé pour vérifier que les logiciels proviennent bien des bonnes personnes, pour protéger les utilisateurs contre le piratage.

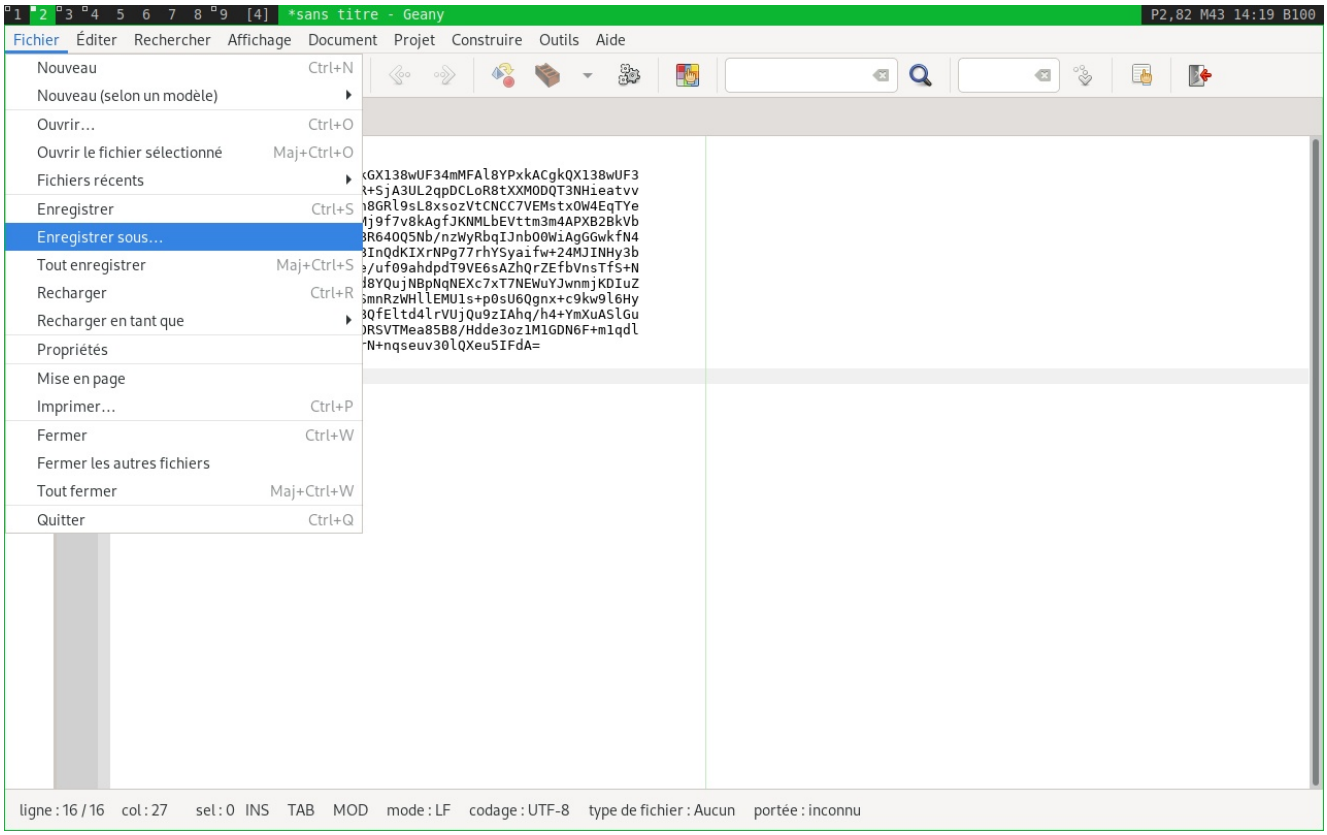



On séléctionne tout le texte, avec "sélectionner tout" ou Ctrl + A, et on copie le texte.

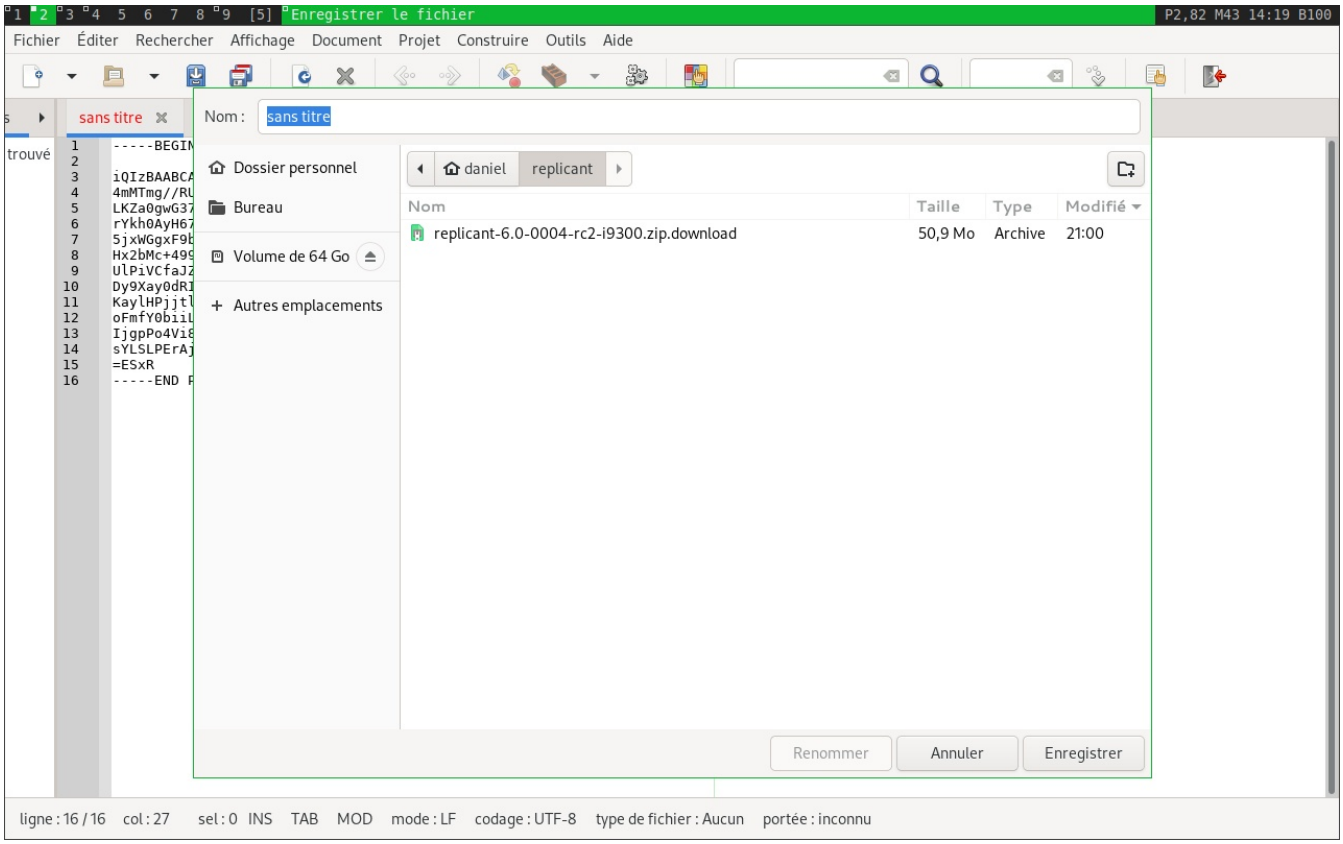



On colle tout ce texte de la signature dans un programme qui s'appelle un éditeur de texte.
L'éditeur de texte n'est pas un traitement de texte, c'est très important.
Il ne travaille que le texte brut non mis en forme. Il faut absolument utiliser ce type de programme.
Il y en a plein: leafpad, geany, medit, gedit, kate, mousepad, ...

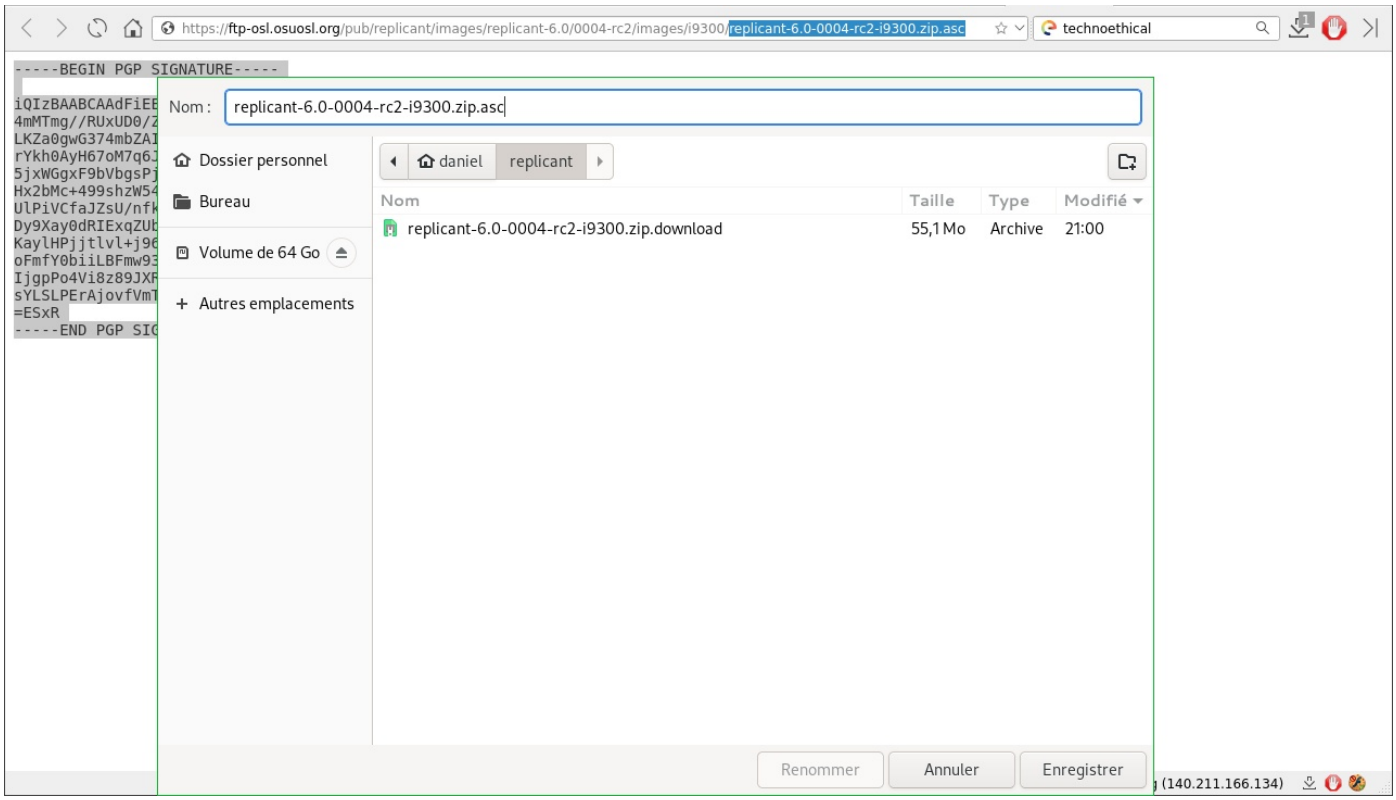
Ici j'utilise geany.



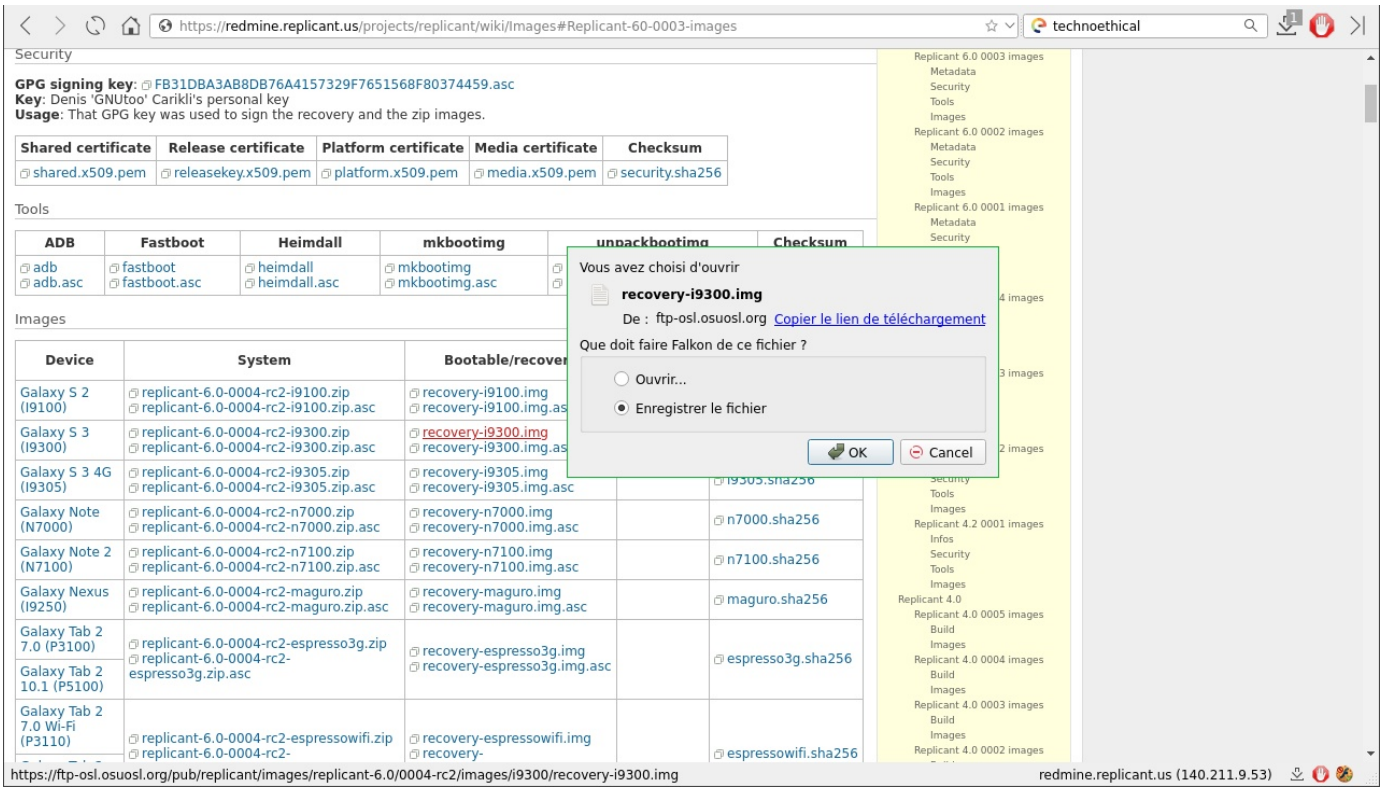

Donc on enregistre sous.
On a avant tout cela créé un dossier replicant où on met tout ce qu'on télécharge.



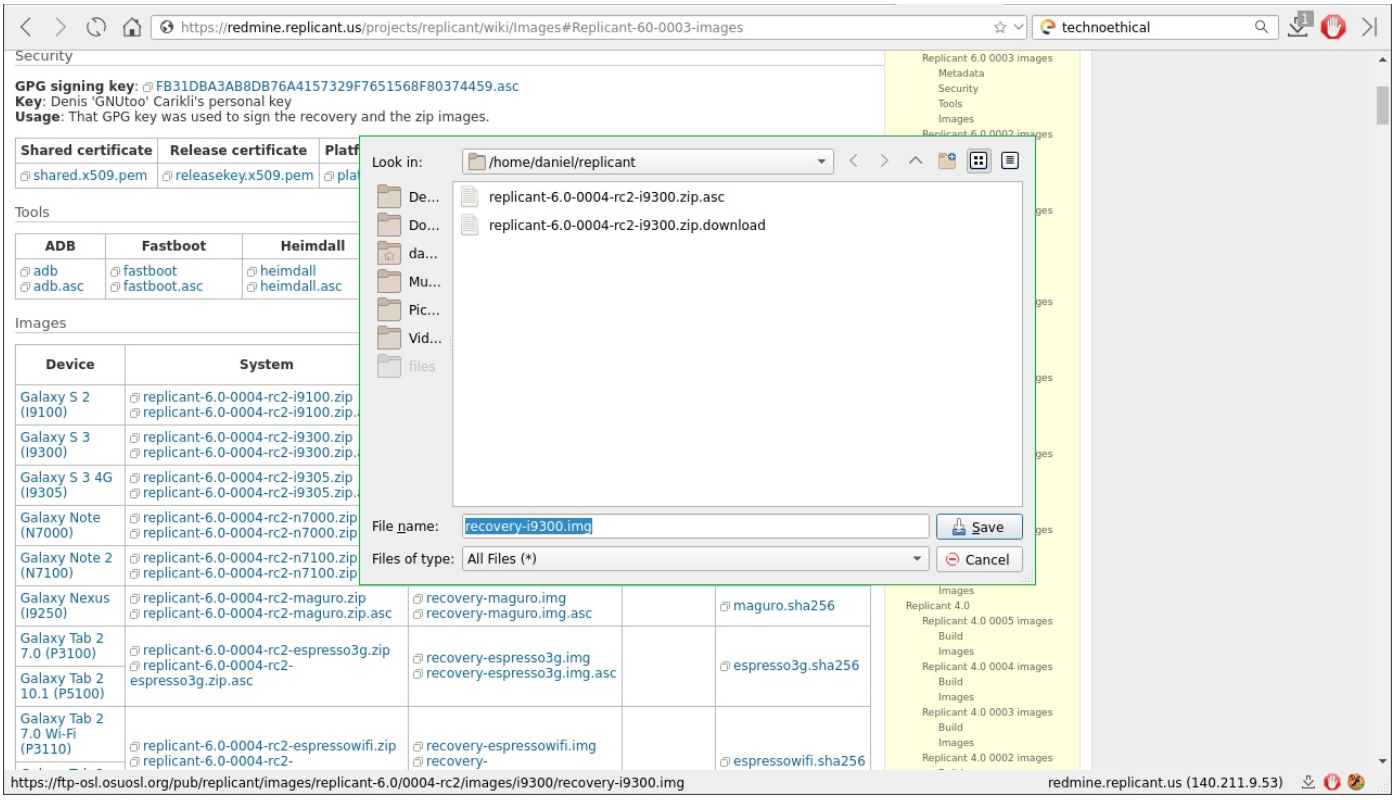

Donc on écrit le nom du fichier (le meme que sur le site).

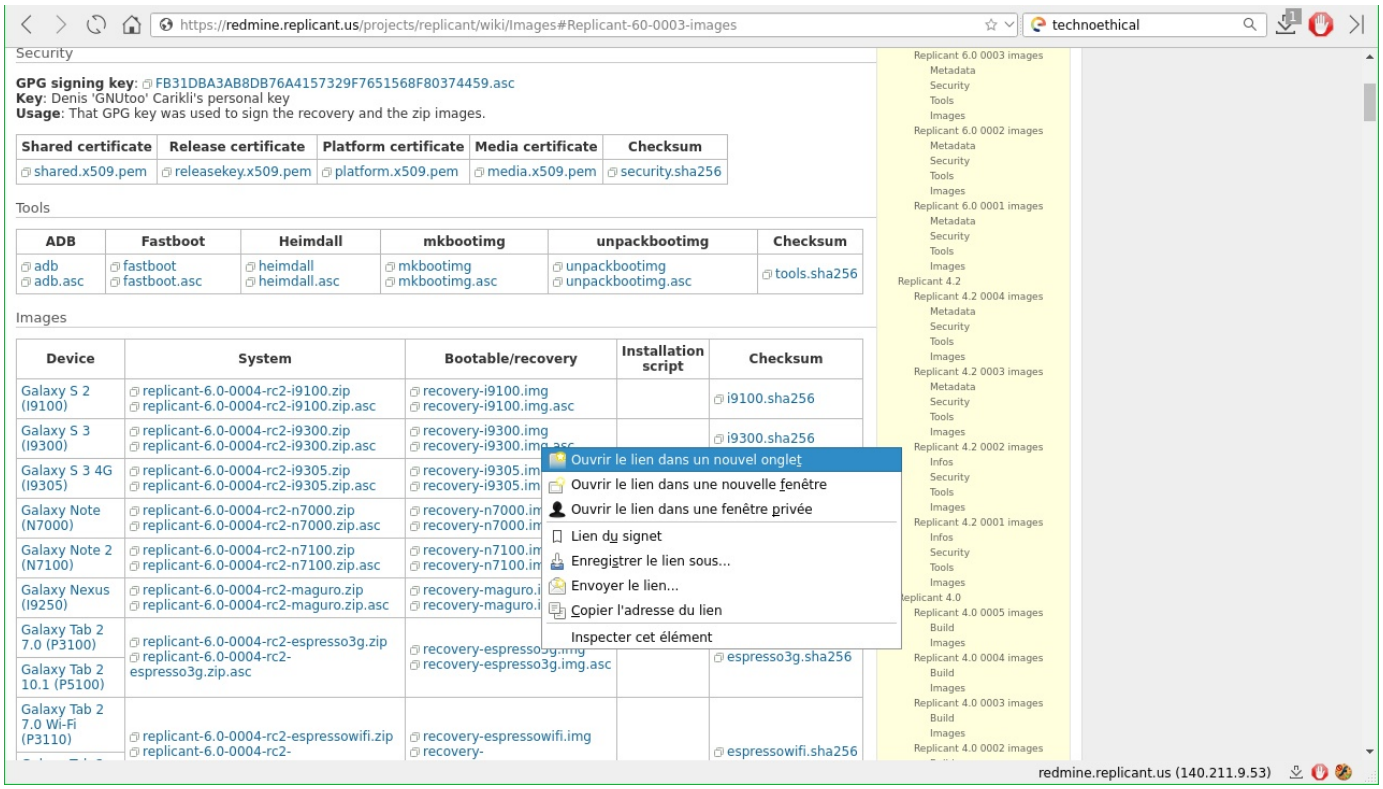



Puis on enregistre.

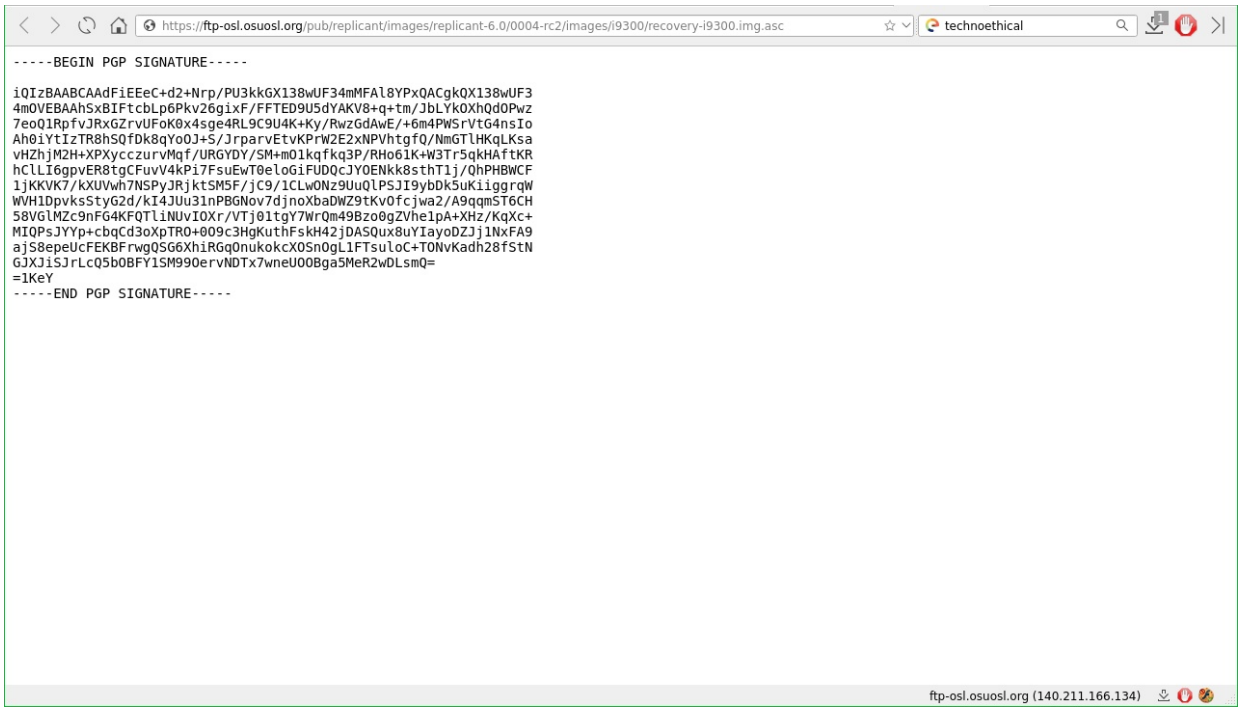



On télécharge le fichier recovery qui va servir à faire démarrer le téléphone sur replicant.

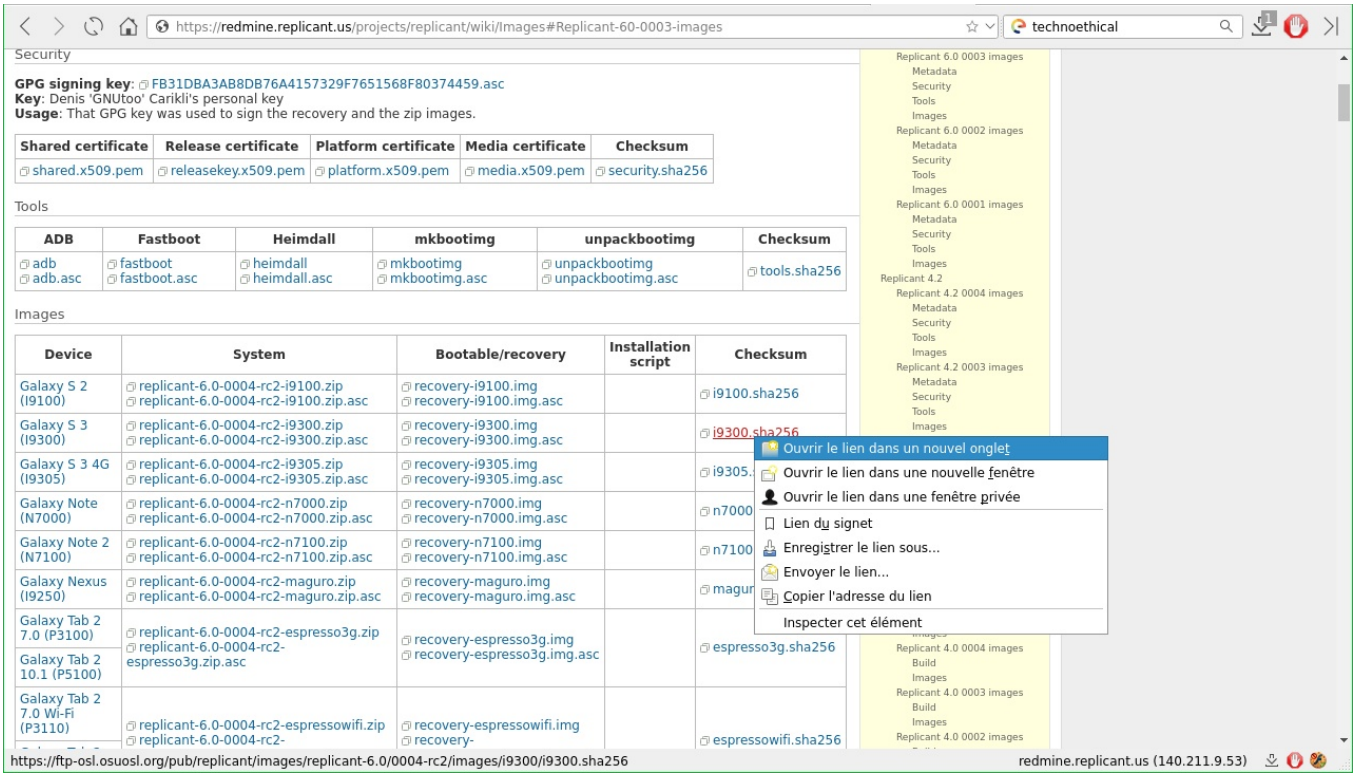


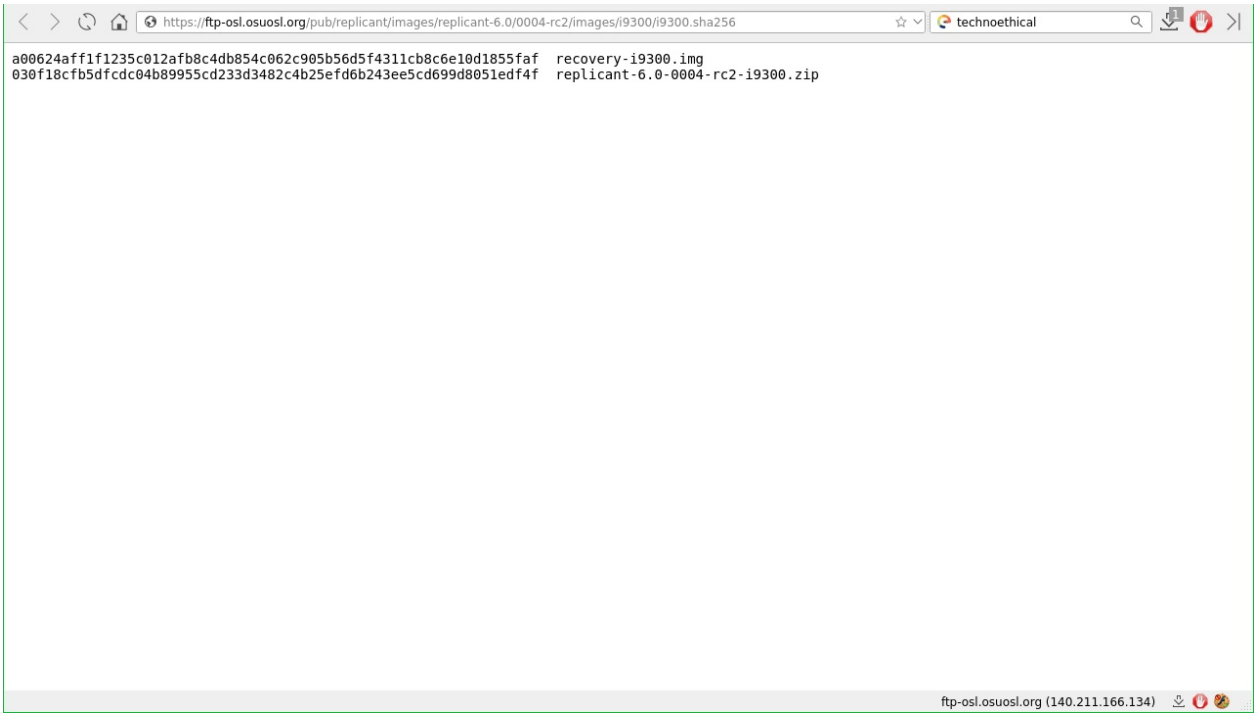

Puis on télécharge le fichier signature correspondant au recovery, de la même manière que pour l'autre fichier .asc.

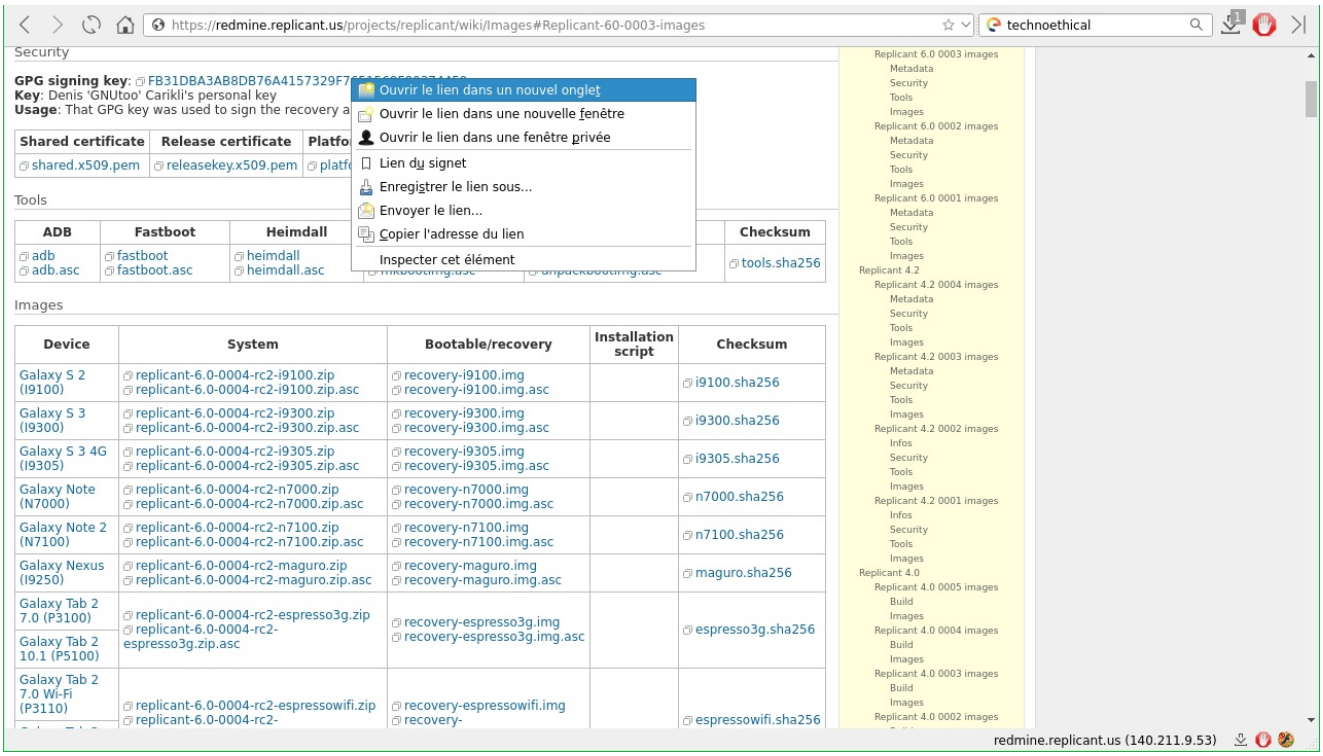



On copie-colle cette signature dans un éditeur de texte, puis on enregistre avec le bon nom: recovery-i9300.asc

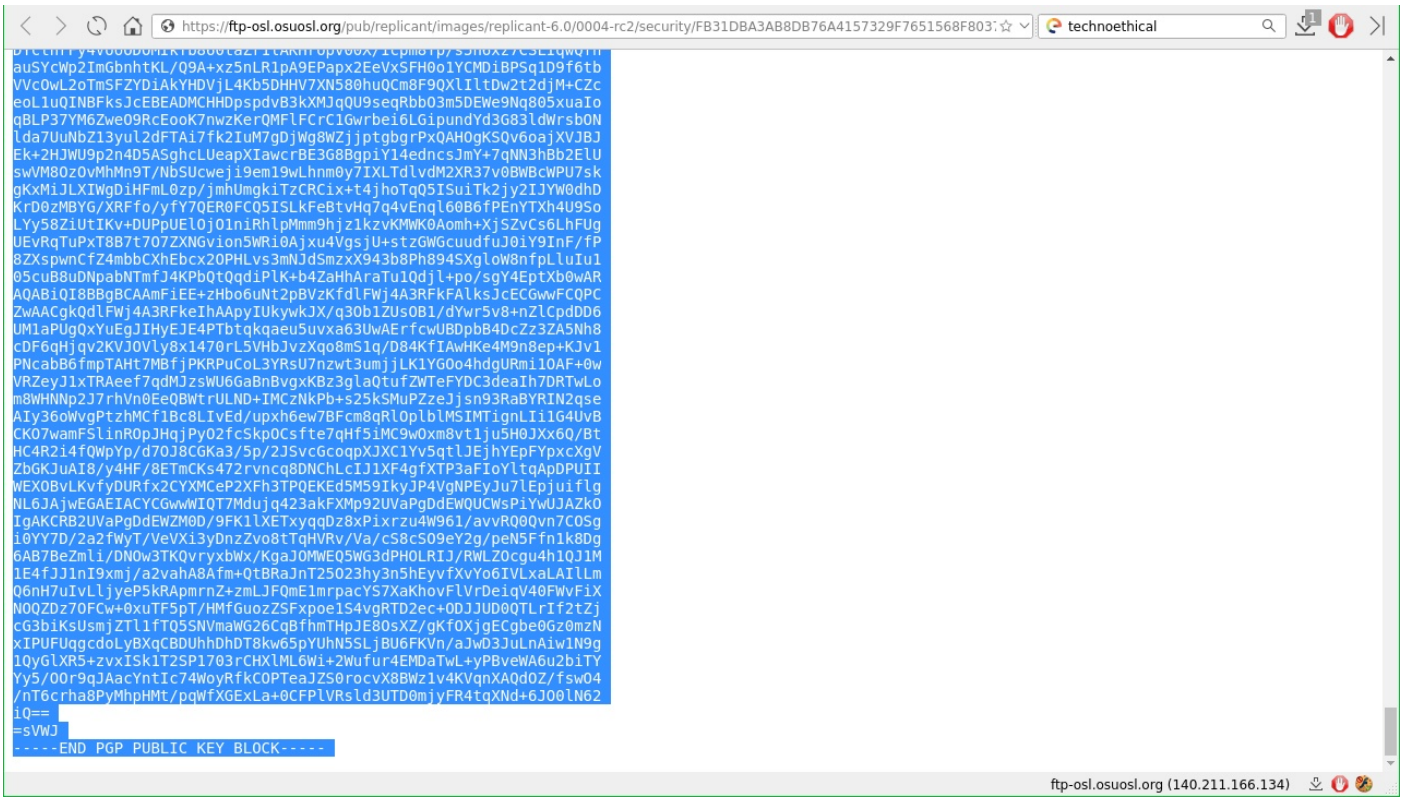


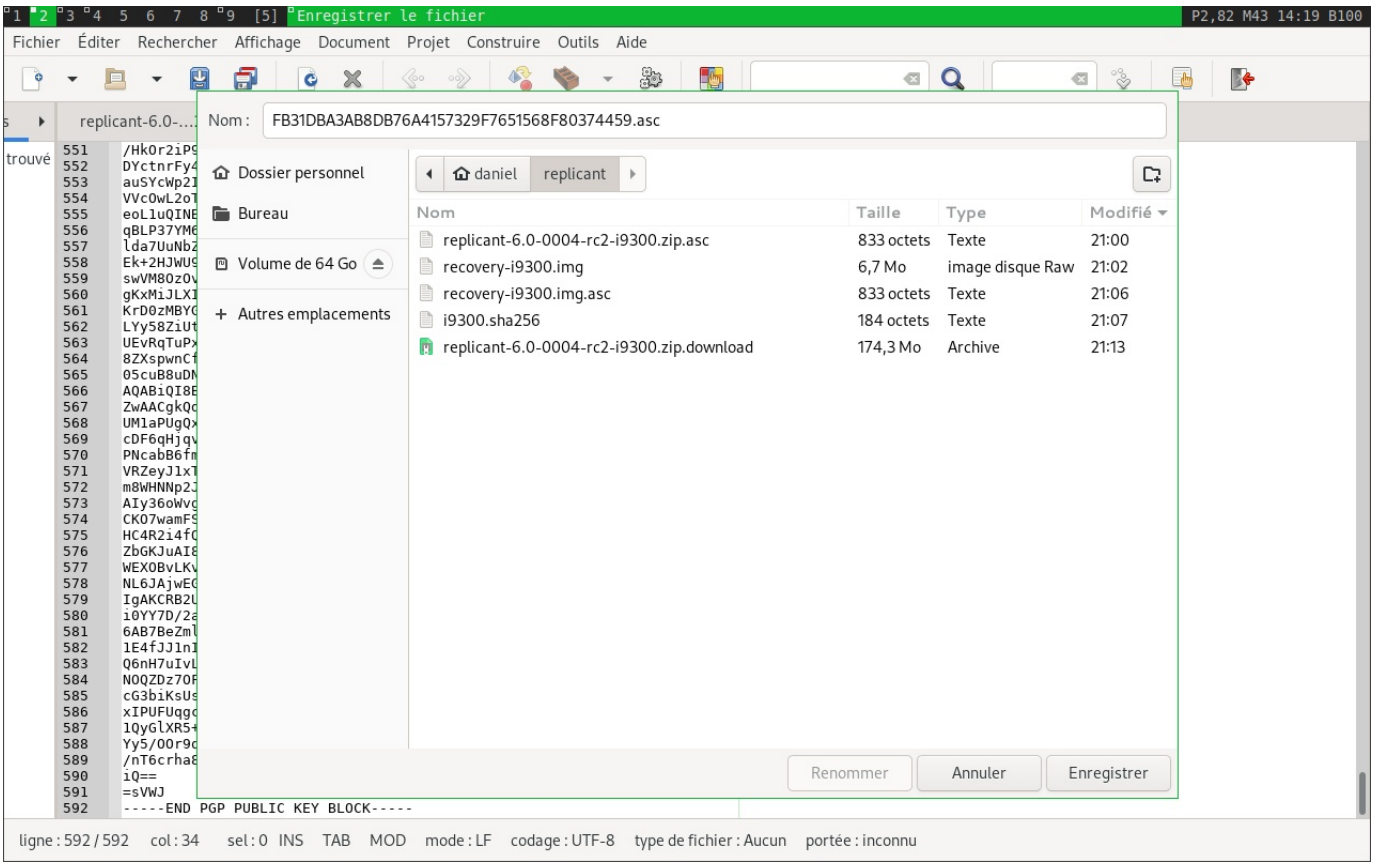

On fait la même chose avec le fichier i9300.sha256
On ouvre dans un nouvel onglet, on on copie-colle le texte dans un éditeur de texte, et on enregistre sous le nom i9300.sha256.



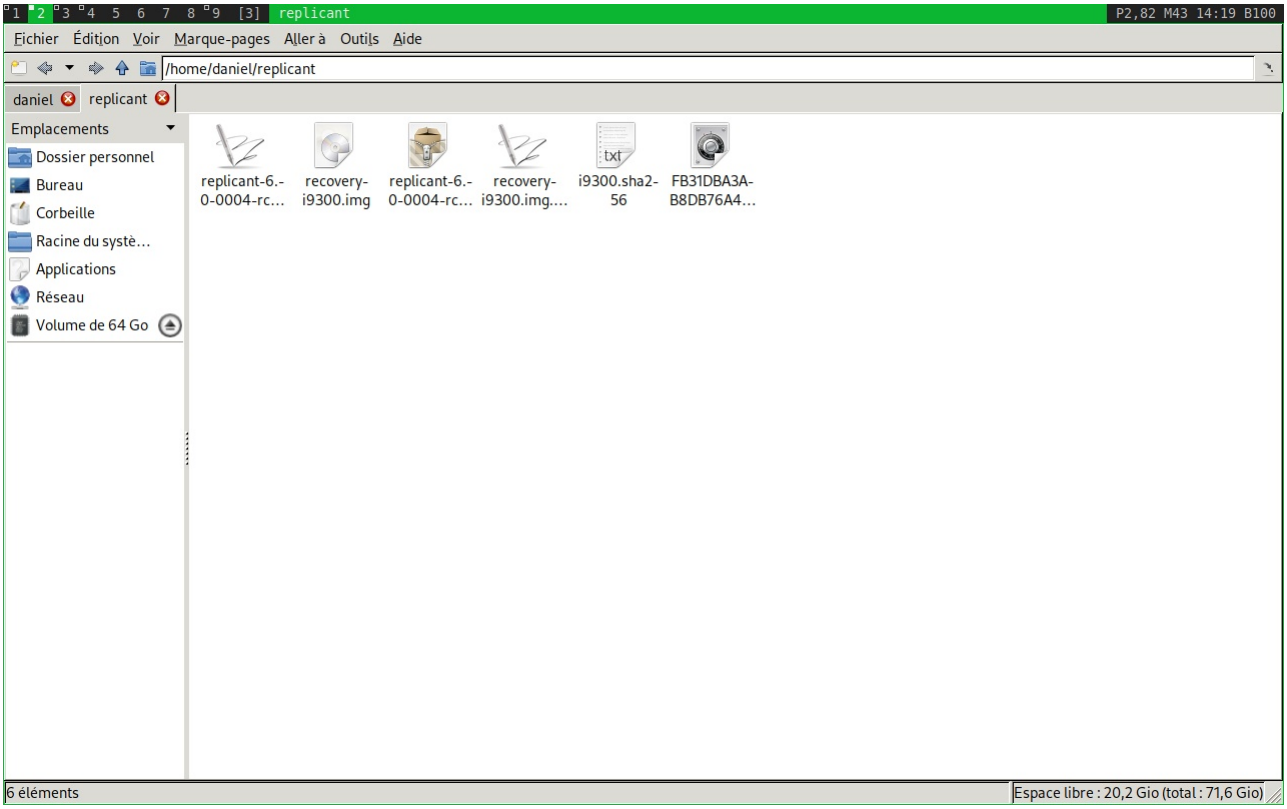

Pareil pour le lien commençant par "FB31", on l'ouvre dans un nouvel onglet, et on copie le texte.
C'est la clé qui permet au développeur de cette version de replicant de signer.



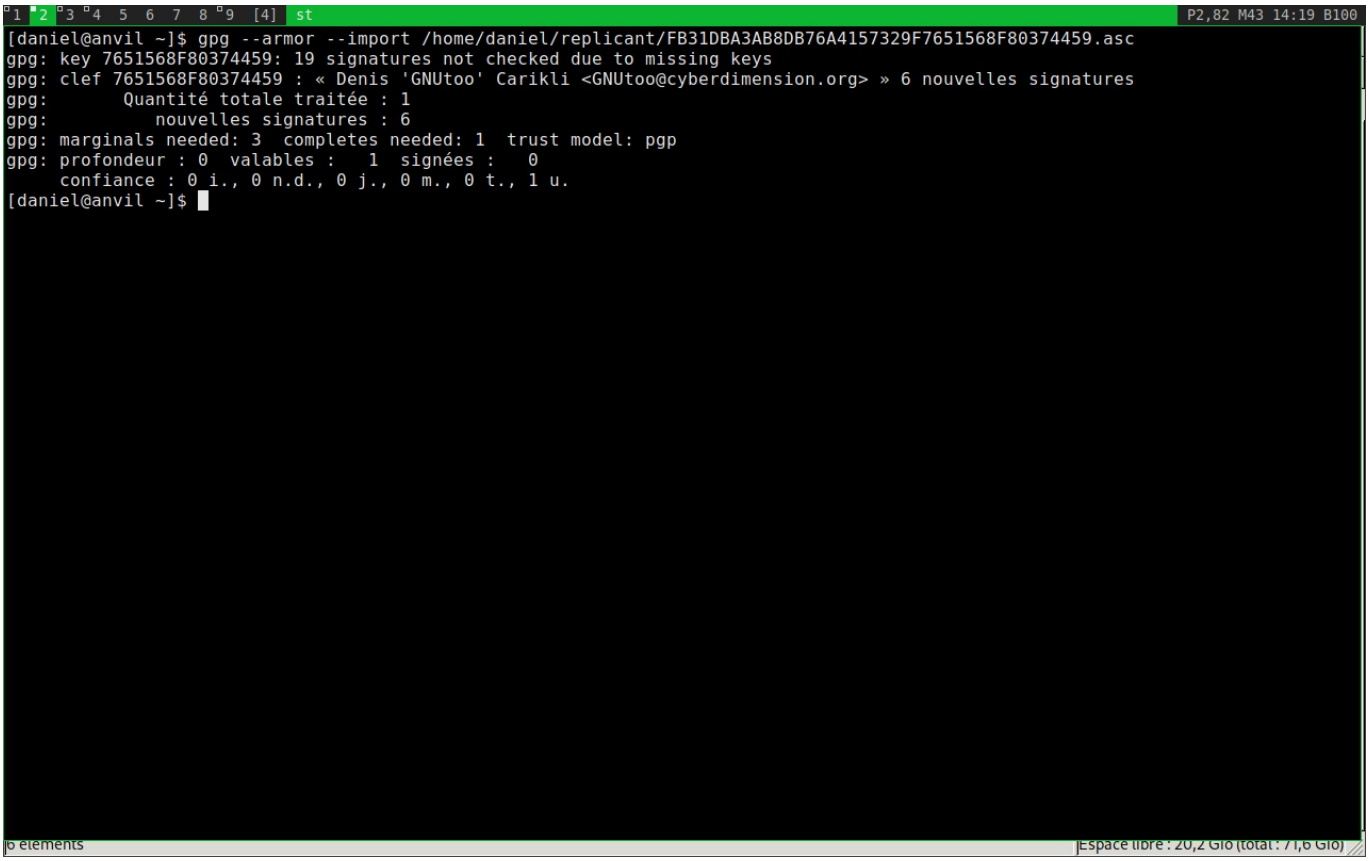




On enregistre sous le nom FB31DBA3AB8DB76A4157329F7651568F80374459.asc qu'on a trouvé dans l'adresse du site commençant par https://ftp-osl.osuosl.org

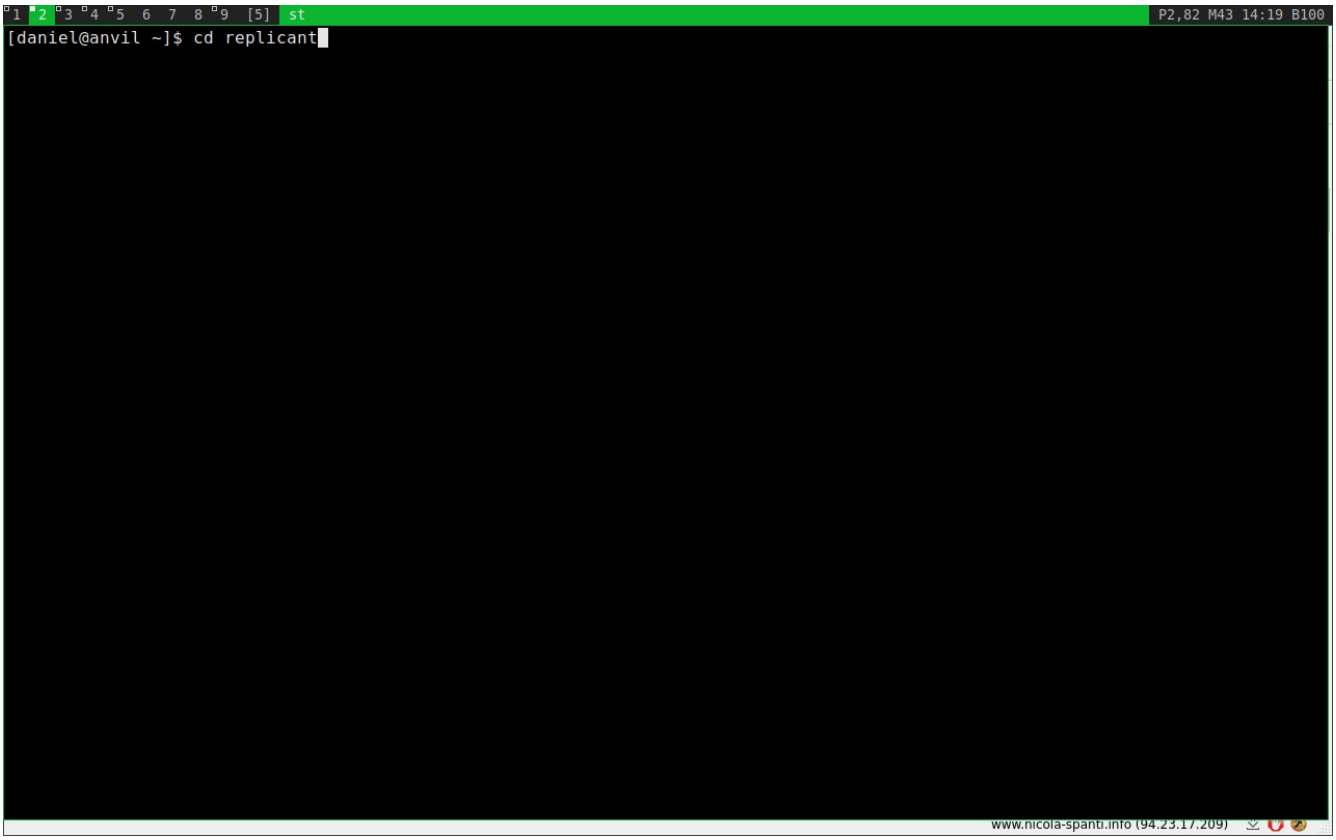
On enregistre ce fichier .asc dans le dossier replicant qu'on a créé auparavant.



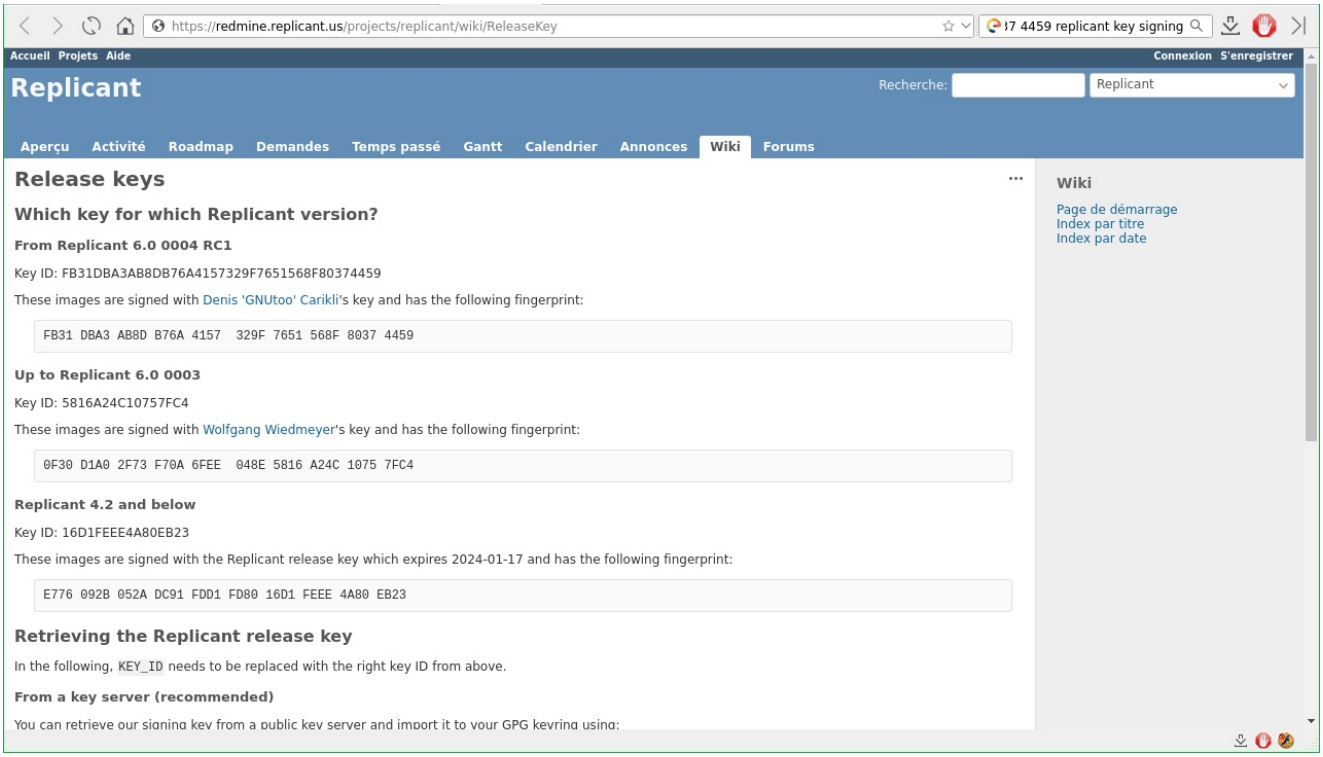

Quand on a tout téléchargé, on a quelque chose qui ressemble à ça. J'utilise le navigateur de fichiers pcmanfm. Donc bien sûr ça peut changer.




À ce stade, on utilise le terminal, et on fait la commande
`gpg --armor --import /home/user/replicant/FB31DBA3AB8DB76A4157329F7651568F80374459.asc`
pour rajouter la clé au trousseau gpg de notre ordinateur.
Les terminaux peuvent avoir plusieurs noms: xterm, konsole, etc… leur icone est souvent un écran noir. Il y a ici un magnifique tuto si jamais vous voulez en savoir plus: https://linuxsurvival.com/




La commande
`cd /chemin/vers/replicant`
permet de se déplacer dans le répertoire replicant qu'on a créé.

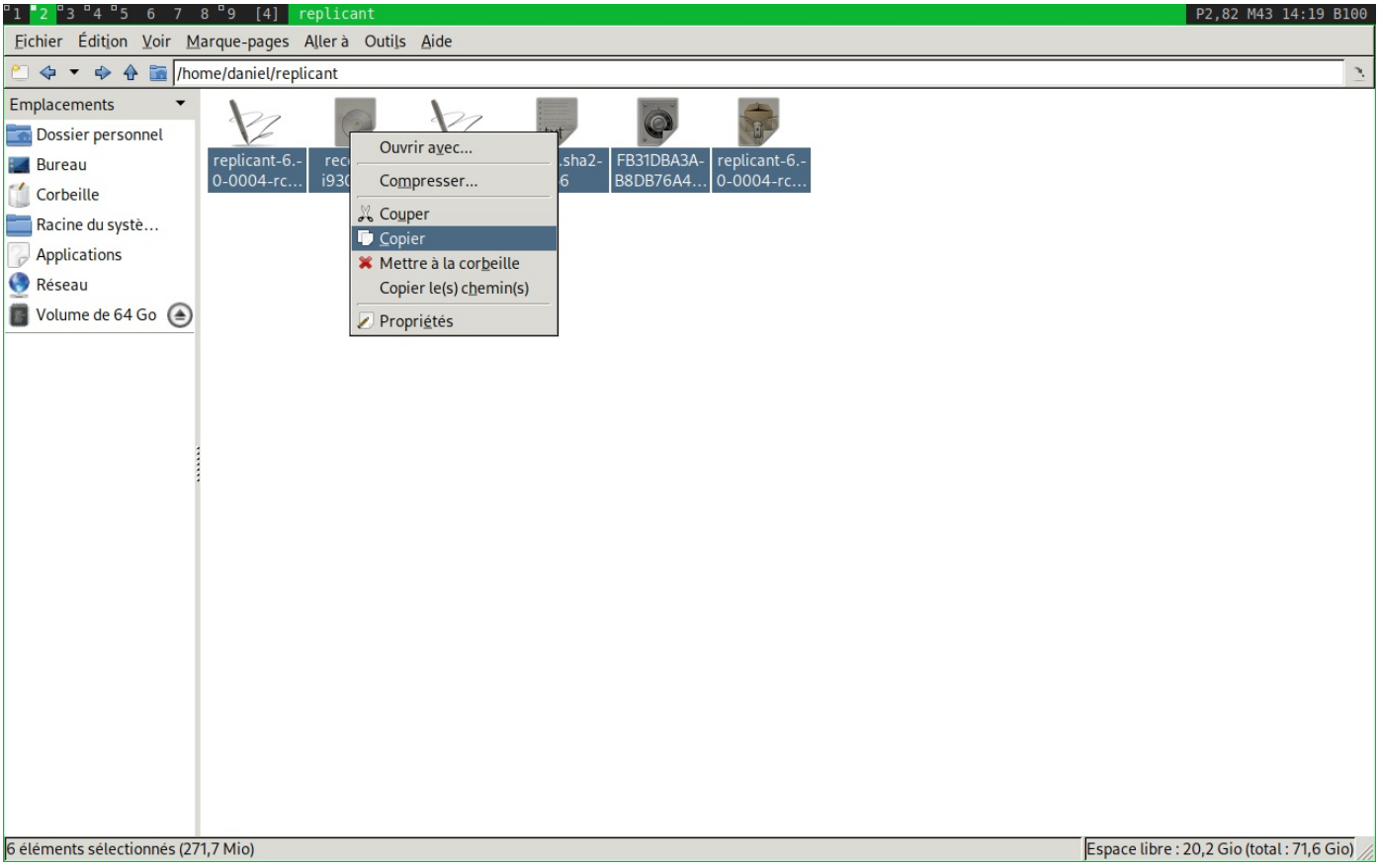



On vérifie sur la page https://redmine.replicant.us/projects/replicant/wiki/ReleaseKey si les codes des clés correspondent bien avec ce qu'on a, puis on lance les commandes de vérification:

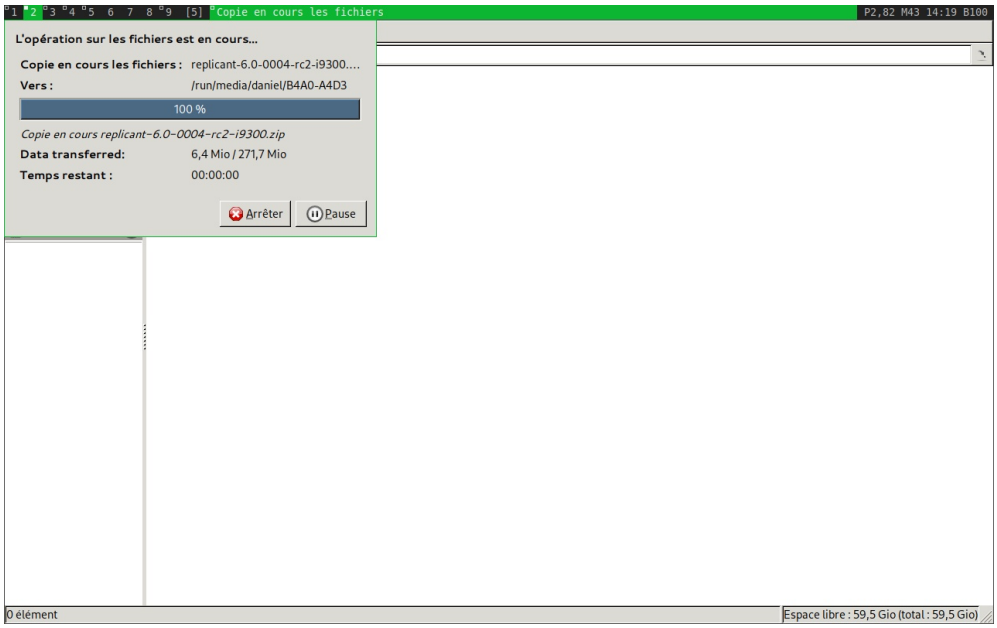
```
gpg --armor --verify chemin/vers/replicant-6.0-i9300.zip.asc
chemin/vers/replicant-6.0-i9300.zip
gpg --armor --verify chemin/vers/recovery.img.asc chemin/vers/
recovery.img
sha256sum -c i9300.sha256
```

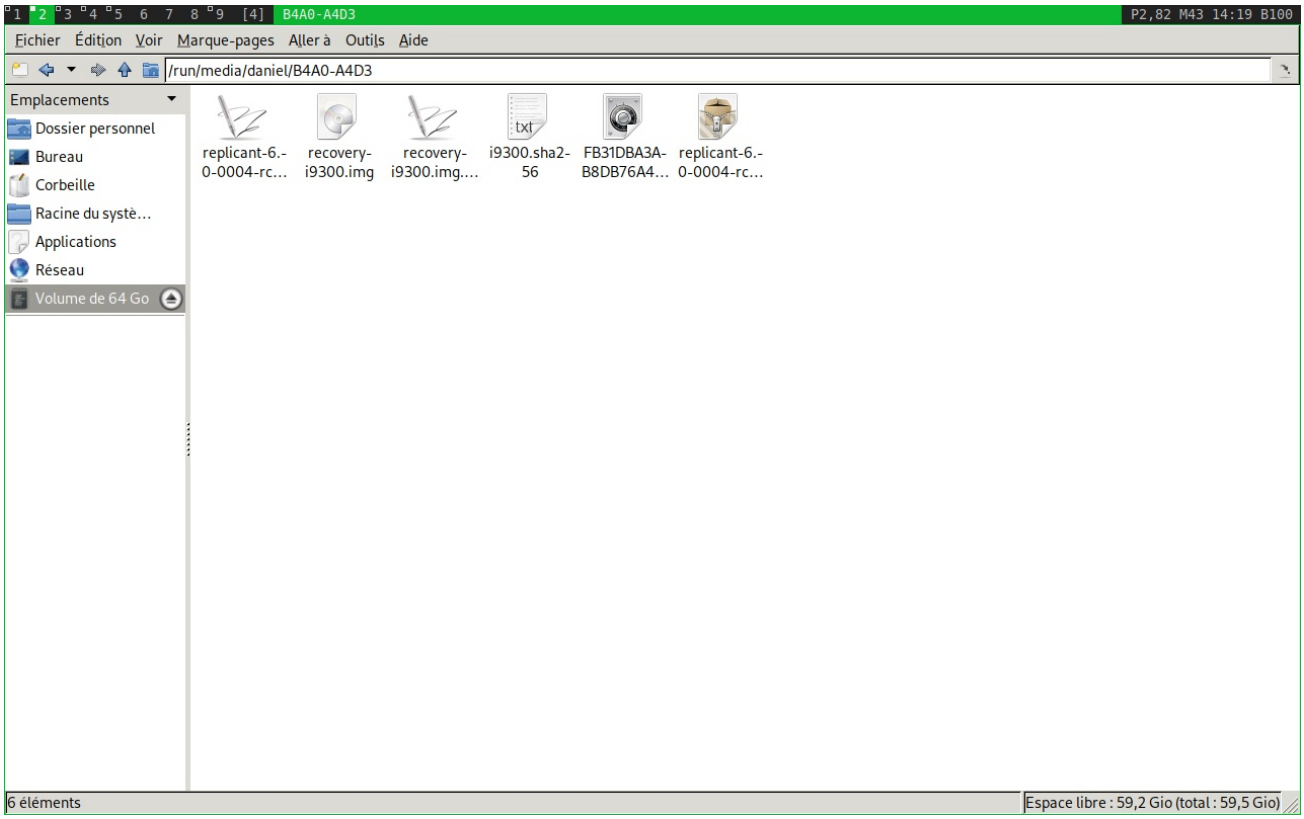
```
[daniel@anvil replicant]$ gpg --armor --verify replicant-6.0-0004-rc2-i9300.zip.asc replicant-6.0-0004-rc2-i9300.zip
gpg: Signature faite le mer. 22 juil. 2020 15:28:57 CEST
gpg:                avec la clef RSA 782F9DDBE36BA7F3D4DE49065F5DFCC14177E263
gpg: Bonne signature de « Denis 'GNUtoo' Carikli <GNUtoo@cyberdimension.org> » [inconnu]
gpg:                 alias « Denis 'GNUtoo' Carikli <GNUtoo@no-log.org> » [inconnu]
gpg:                 alias « Denis 'GNUtoo' Carikli <GNUtoo@riseup.net> » [inconnu]
gpg:                 alias « Denis 'GNUtoo' Carikli <GNUtoo@makefreedom.org> » [inconnu]
gpg: Attention : cette clef n'est pas certifiée avec une signature de confiance.
gpg:             Rien n'indique que la signature appartient à son propriétaire.
Empreinte de clef principale : FB31 DBA3 AB8D B76A 4157  329F 7651 568F 8037 4459
   Empreinte de la sous-clef : 782F 9DDB E36B A7F3 D4DE  4906 5F5D FCC1 4177 E263
[daniel@anvil replicant]$ gpg --armor --verify recovery-i9300.img.asc recovery-i9300.img
gpg: Signature faite le mer. 22 juil. 2020 15:28:52 CEST
gpg:                avec la clef RSA 782F9DDBE36BA7F3D4DE49065F5DFCC14177E263
gpg: Bonne signature de « Denis 'GNUtoo' Carikli <GNUtoo@cyberdimension.org> » [inconnu]
gpg:                 alias « Denis 'GNUtoo' Carikli <GNUtoo@no-log.org> » [inconnu]
gpg:                 alias « Denis 'GNUtoo' Carikli <GNUtoo@riseup.net> » [inconnu]
gpg:                 alias « Denis 'GNUtoo' Carikli <GNUtoo@makefreedom.org> » [inconnu]
gpg: Attention : cette clef n'est pas certifiée avec une signature de confiance.
gpg:             Rien n'indique que la signature appartient à son propriétaire.
Empreinte de clef principale : FB31 DBA3 AB8D B76A 4157  329F 7651 568F 8037 4459
   Empreinte de la sous-clef : 782F 9DDB E36B A7F3 D4DE  4906 5F5D FCC1 4177 E263
[daniel@anvil replicant]$ sha256sum -c i9300.sha256
recovery-i9300.img: Réussi
replicant-6.0-0004-rc2-i9300.zip: Réussi
[daniel@anvil replicant]$
```

Résultat.
La signature est correcte, mais le programme dit qu'on n'est pas sûr de l'appartenance. Le développeur utilise une sous-clé. Le site internet dit que la clé principale est bien la bonne.
Ce qui est intéressant c'est qu'on a les mails de Denis 'GNUtoo" Carikli pour vérifier. Il est aussi sur le forum ( https://redmine.replicant.us/projects/replicant/boards ), et donc on peut poser la question.

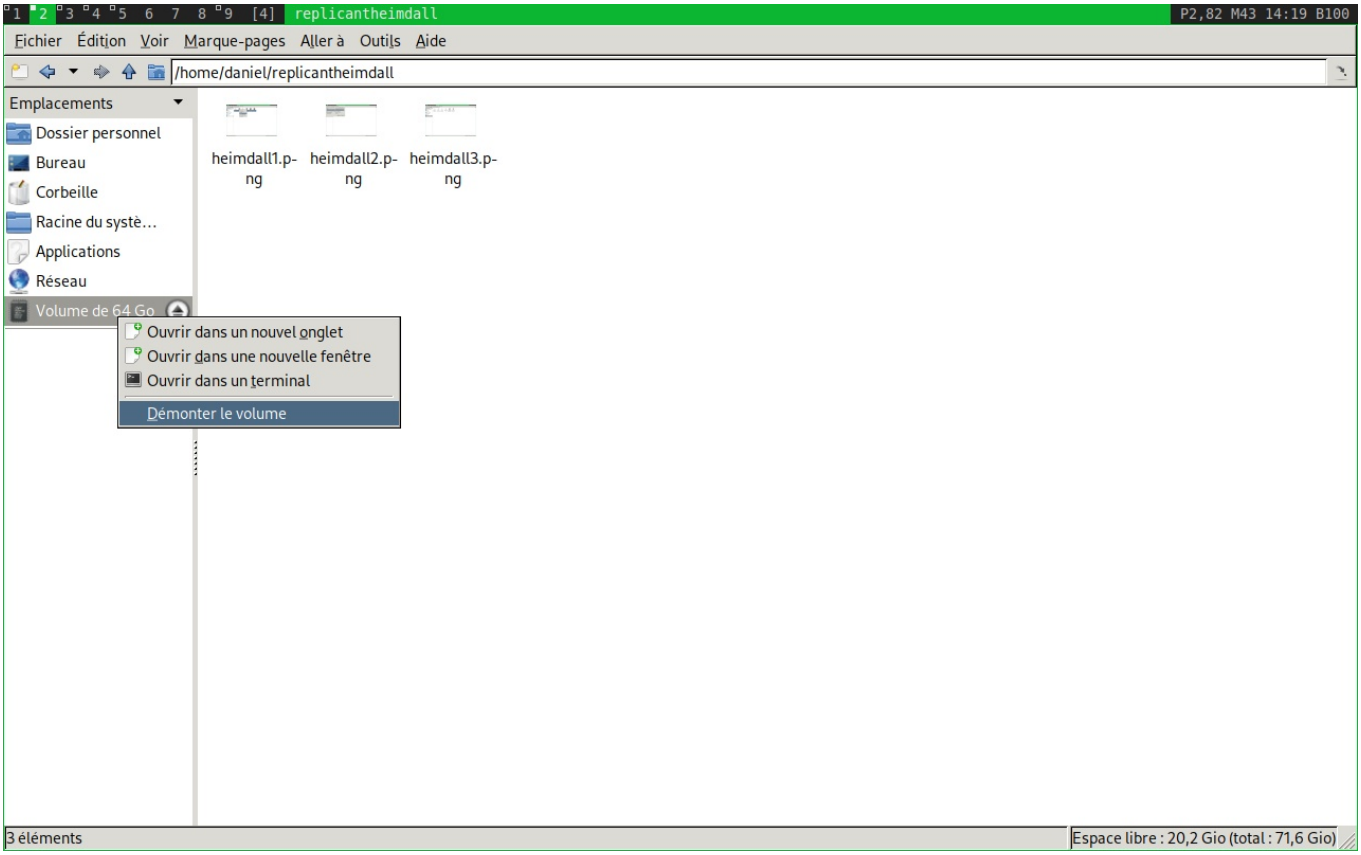


On va copier-coller le contenu du dossier replicant avec tout ce qu'on a téléchargé sur la carte microSD qu'on a formaté juste avant.

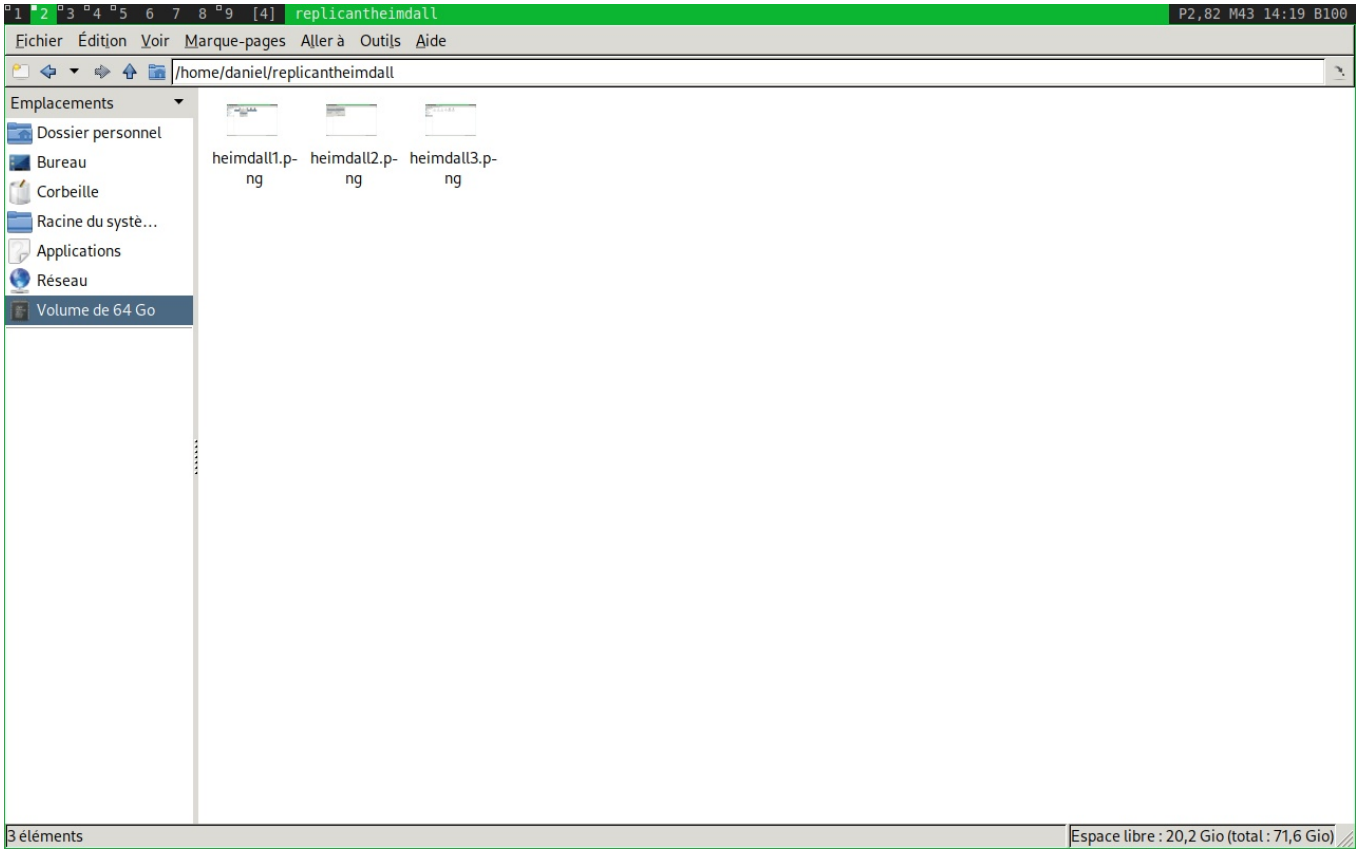



On a tous les fichiers qui ont été copiés.
Les fichiers de signature et de vérification en .asc ou en .sha256 ne sont pas forcément utiles pour l'installation sur le téléphone proprement dite, je les garde par précaution, on pourra toujours les effacer après.

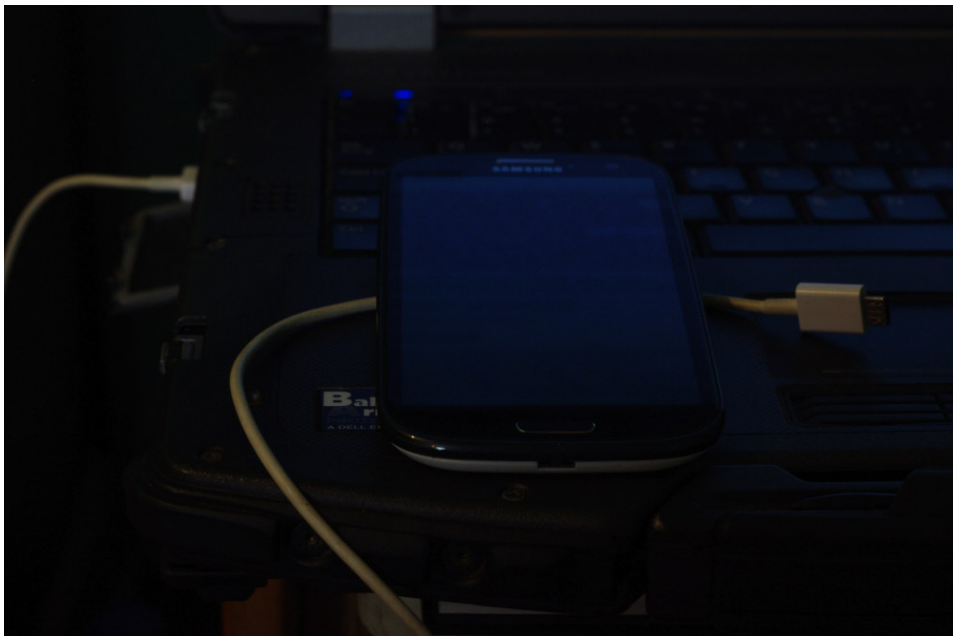



On démonte la clé en faisant clic droit "démonter le volume".




Volume démonté.

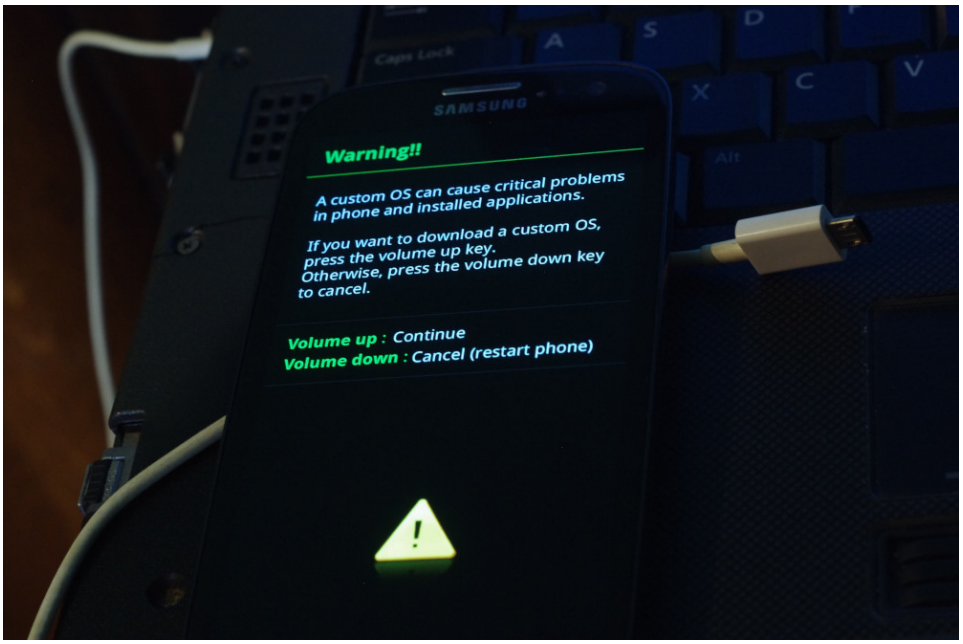
On insère la carte microSD dans le téléphone.



Quand le téléphone est débranché et éteint, on appuie simultanément sur les touches volume bas, la touche "maison" ou home (la touche centrale du bas), et la touche pour allumer et éteindre.

Un message d'avertissement apparaît.

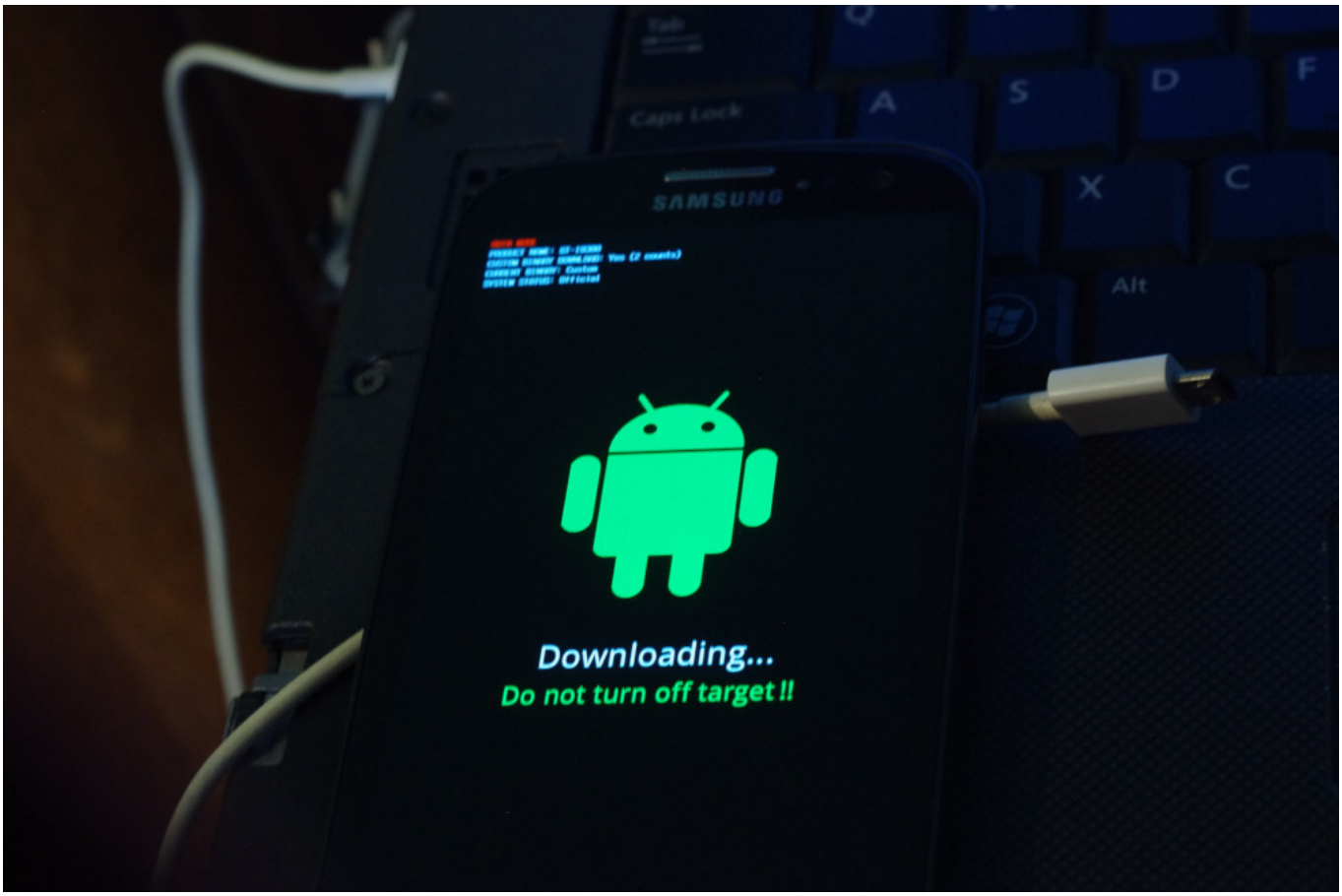
On appuie sur la touche volume haut pour confirmer.



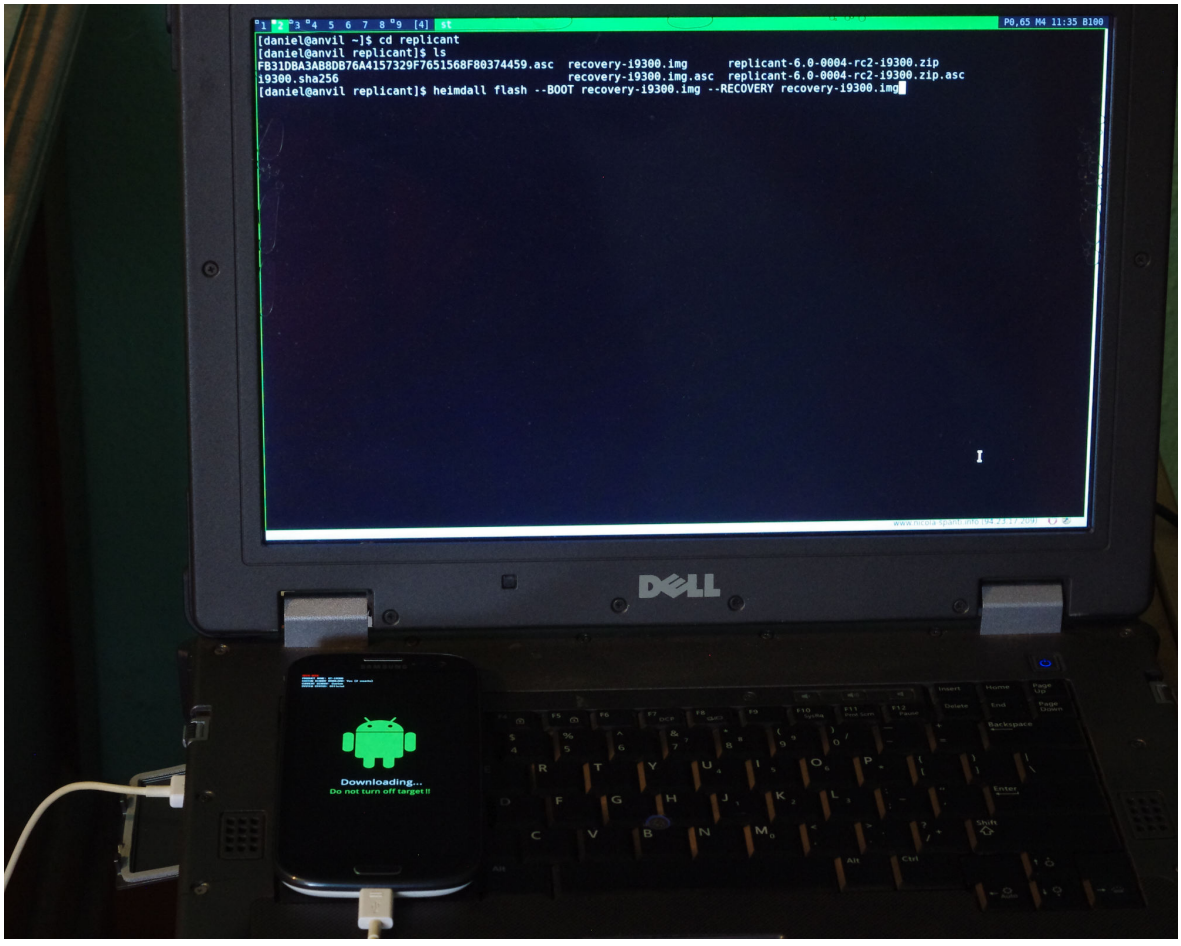

Il est mieux pour toutes ces opérations d'utiliser les touches plutôt que l'écran tactile, cela évite de faire des fausses manipulations.

On aura besoin pour la suite d'avoir heimdall installé sur l'ordinateur. C'est le programme qui sert à "flasher" le téléphone pour y installer replicant.

https://www.glassechidna.com.au/heimdall/




On arrive là. À ce stade on branche le câble usb qui relie l'ordi au téléphone.
Tous les câbles de chargeurs ne sont pas équivalents, certains ne transmettent pas les données, et donc il peut y avoir des drôles de messages d'erreurs.
S'assurer d'avoir un bon câble.



Donc dans le terminal, on fait:

```
cd /chemin/vers/replicant
```

Pour aller dans le dossier qu'on a créé et dans lequel il y a tout ce qu'on a téléchargé.
Puis:

```
ls
```

Pour vérifier s'il y a bien tout dans le dossier replicant.
Puis:

```
heimdall flash --BOOT recovery-i9300.img --RECOVERY recovery-i9300.img
```

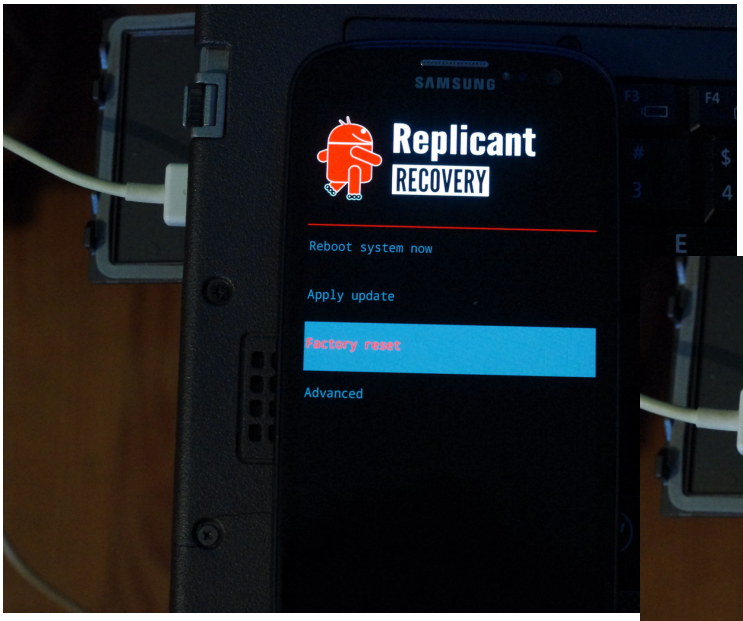
Pour installer dans le téléphone ce fichier système qui lui permet de démarrer.


Résultat.
Aucun message d'erreur tout s'est parfaitement bien passé.


L'appareil, après la commande heimdall réussie, redémarre, et on arrive à cet écran.

On va supprimer les données du téléphone. C'est nécessaire pour toutes les installations de ce type, ou pour la réinitialisation du téléphone.

On sélectionne "Factory reset".




Puis on sélectionne "Wipe data (keep media)"

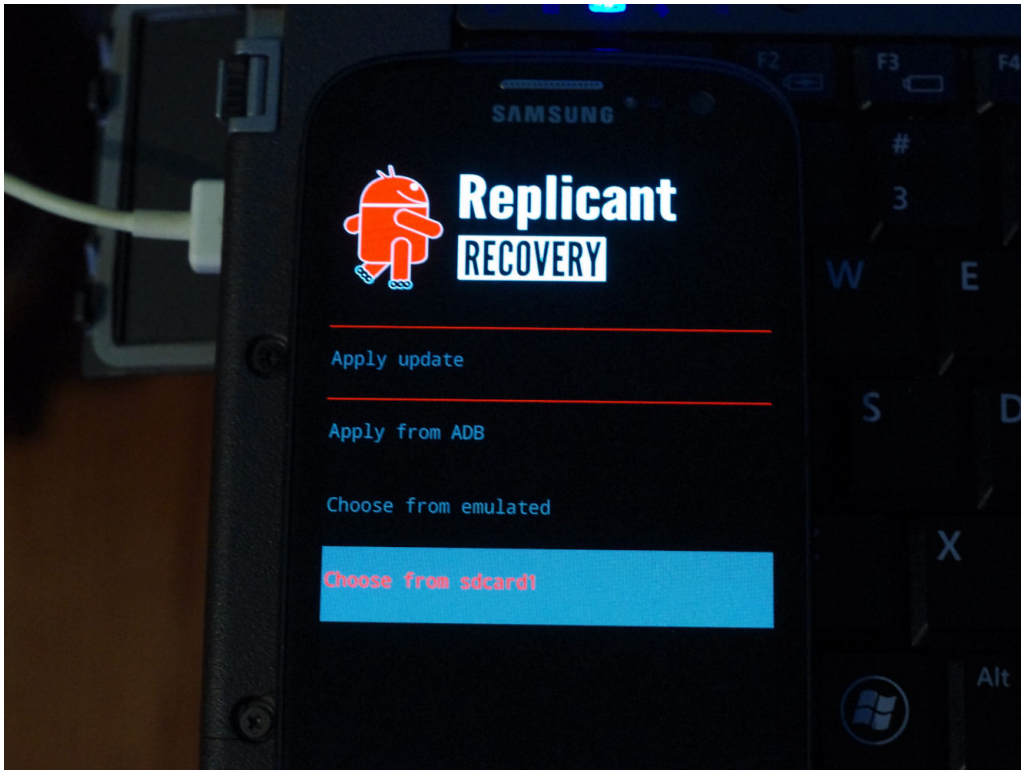
On confirme en sélectionnant "Yes"



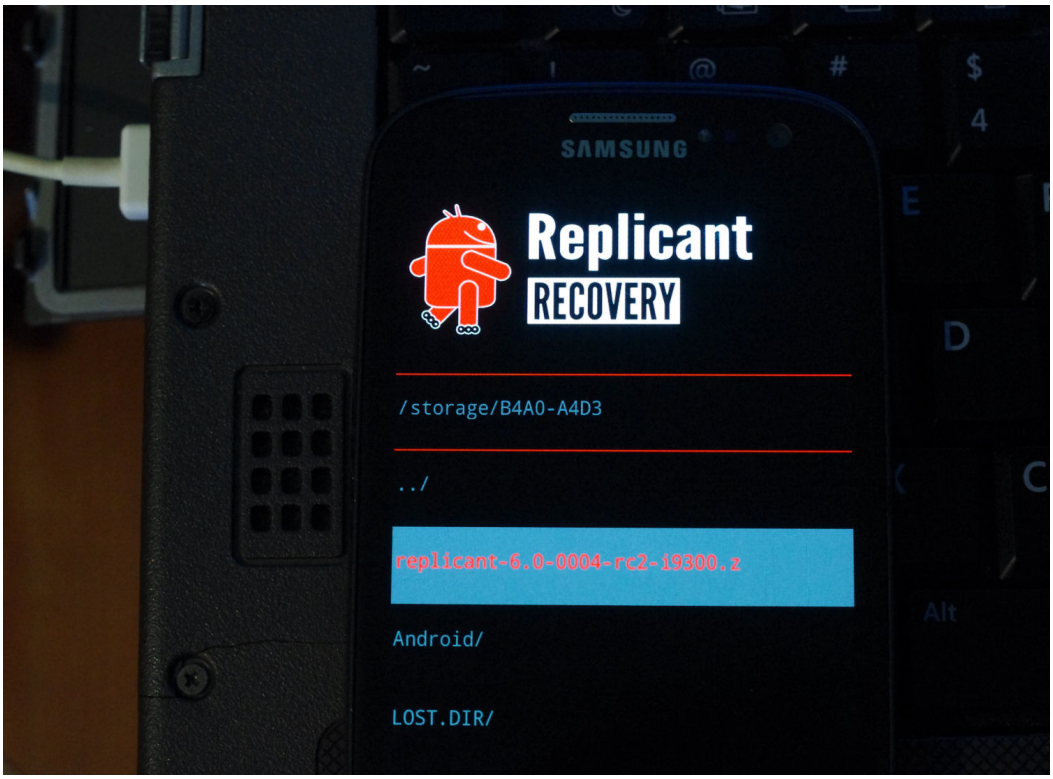
Les données utilisateur ne sont pas que les documents et fichiers personnels, mais aussi tous les réglages des programmes, les sms non sauvegardés dans la carte SIM, un certain nombre de programmes installés, etc...


On retourne à cet écran (faire précédent avec la touche retour si nécessaire).

On sélectionne "Apply update".

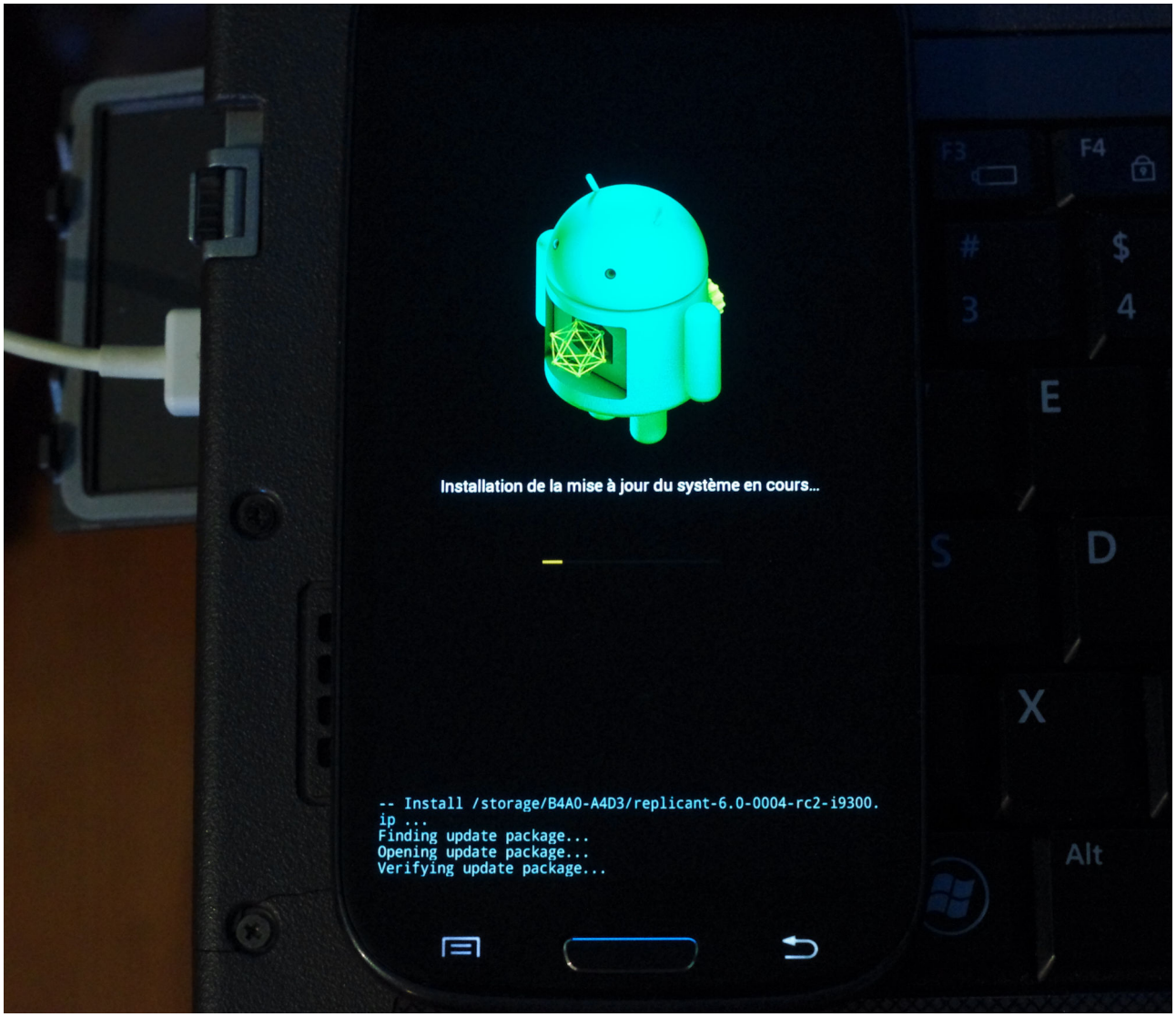



On choisit "Choose from sdcard", pour pouvoir installer le système (qui est le fichier en .zip) dans le téléphone.



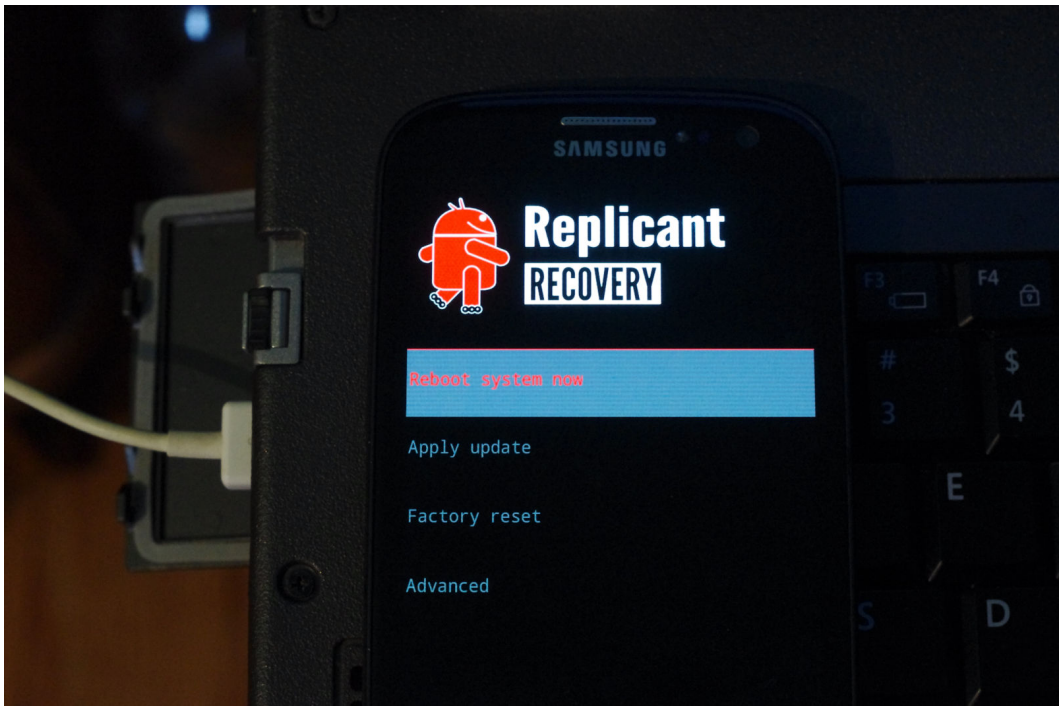

Puis on choisit replicant-6.0-004-rc2-i9300...

Dans votre cas ça sera replicant-6.0-i9300.zip, ou alors la version conseillée la plus récente.



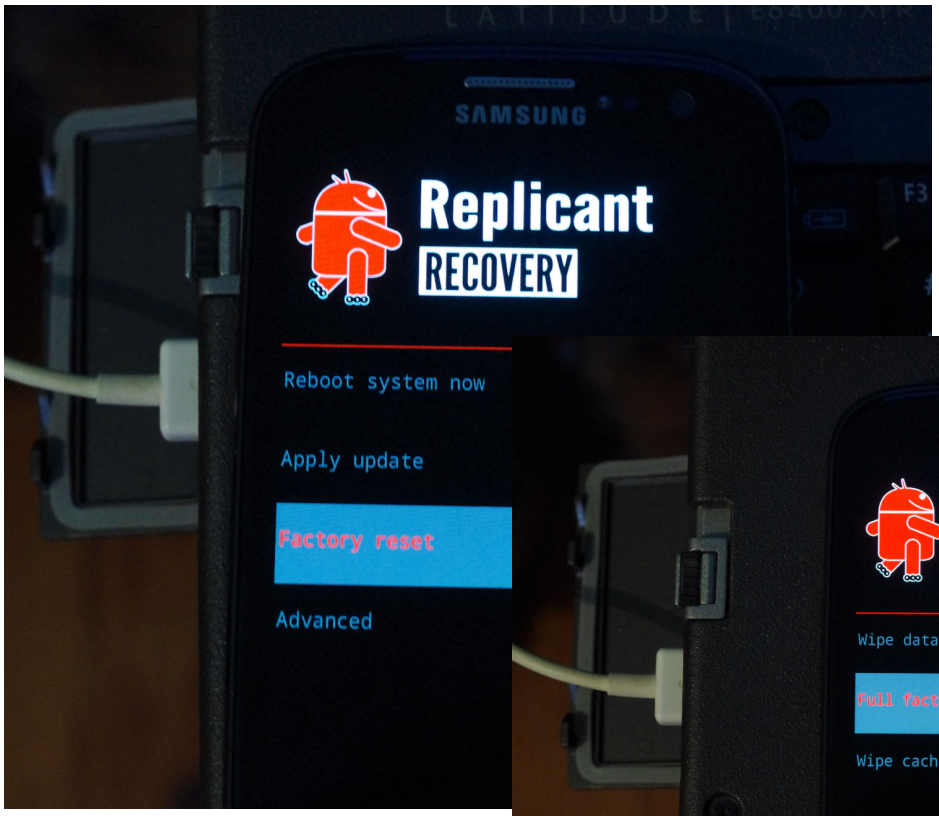

L'installation prend un peu de temps.

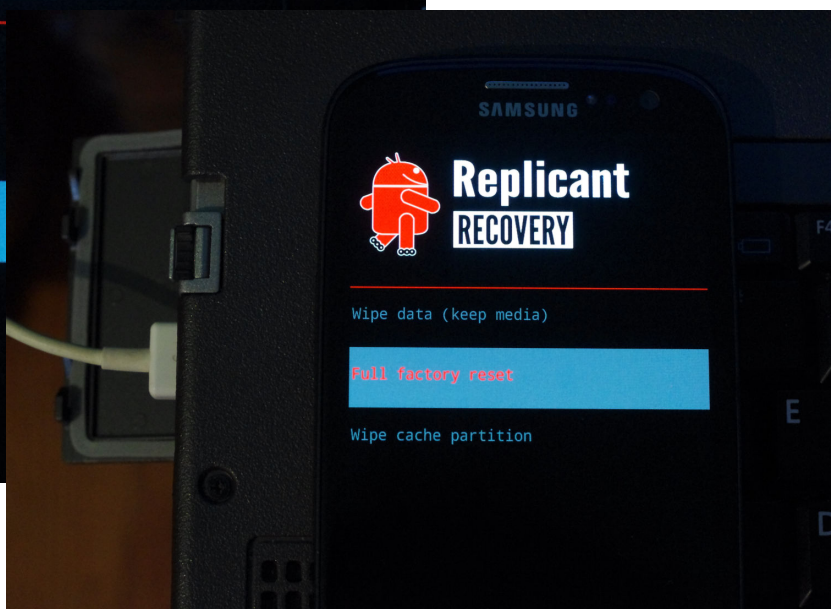
Replicant est à l'origine dérivé d'un Android libre (Android Open Source Project), puis de LineageOS, donc les logos et la présentation ressemblent souvent.




Après l'installation du système, on arrive ici.

Il faut ensuite faire la réinitialisation d'usine.
On séléctionne "Factory reset"



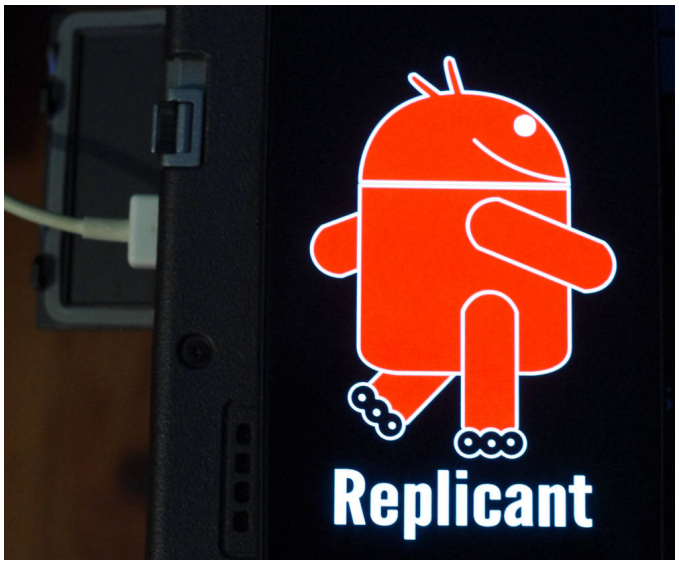




On choisit "Full factory reset"


Puis on confirme en choisissant "Yes"


Choisissez "Reboot system now" pour démarrer replicant.

L'installation est terminée et le démarrage sera particulier car ce sera un premier démarrage, où il demande un certain nombre d'infos.


Les deux écrans de démarrage typiques, qu'on aura à chaque fois qu'on démarre le téléphone. Quand on s'en sert, bien penser à l'éteindre de temps en temps, ou de le redémarrer.

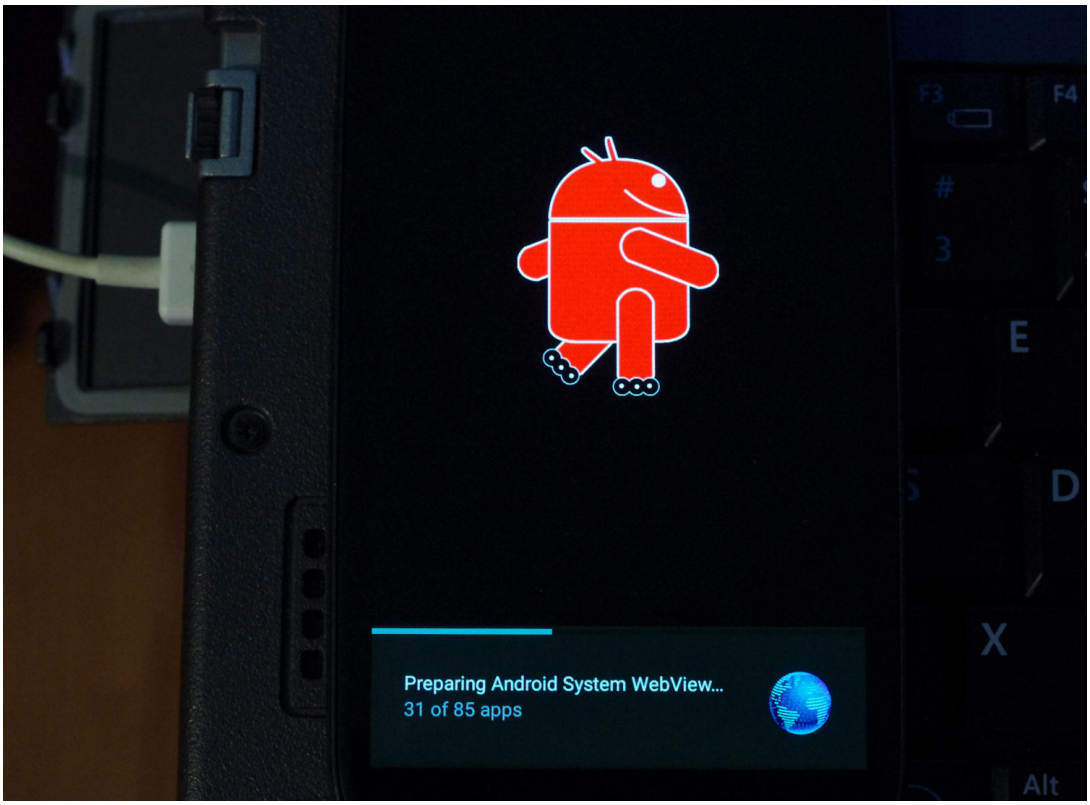
En fait s'il reste allumé sans interruption pendant des semaines il finit par devenir lent puis ne plus bien marcher.

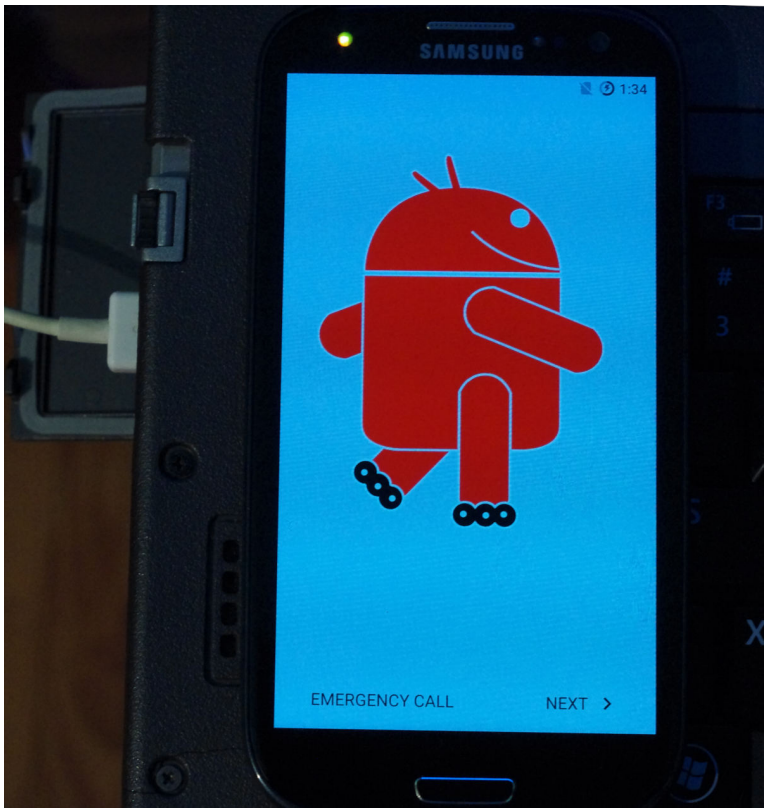
Bien utiliser le bouton d'éteignage à droite en faisant un appui long si on veut démarrer son téléphone normalement.

On peut démarrer son téléphone en mode sécurisé (ne charge que les programmes de base de l'installation de replicant). Ce mode est utile pour permettre au téléphone de fonctionner et démarrer même si un programme a perturbé le démarrage normal.

Pour démarrer dessus, attendre que le logo replicant apparaîsse, puis appuyer sur la touche volume bas jusqu'à ce qu'on ne le voie plus.

Ce mode peut être activé par erreur si quelque chose appuie sur le bouton volume pendant le démarrage (ce qui m'est arrivé avec une housse que j'ai bricolé). Un redémarrage permet de revenir au mode normal.

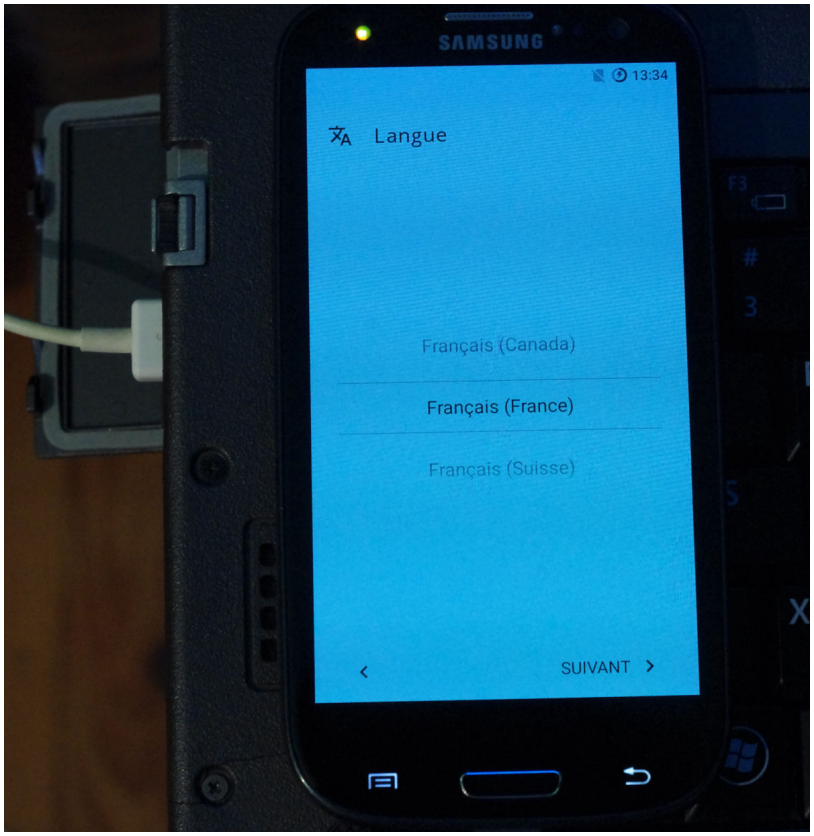



Le démarrage passe en revue toutes les "applications", puis on arrive à l'écran d'accueil du premier démarrage.

On peut passer à un appel d'urgence, ou alors commencer à faire les principaux réglages de base du système.

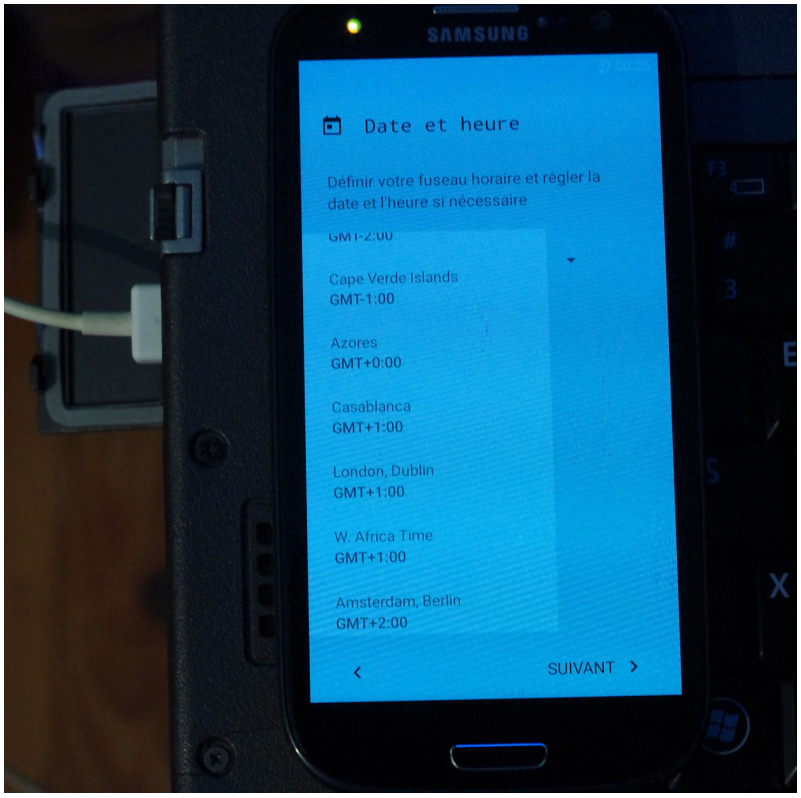
On appuie sur "Next"




On choisit la langue principale du système.

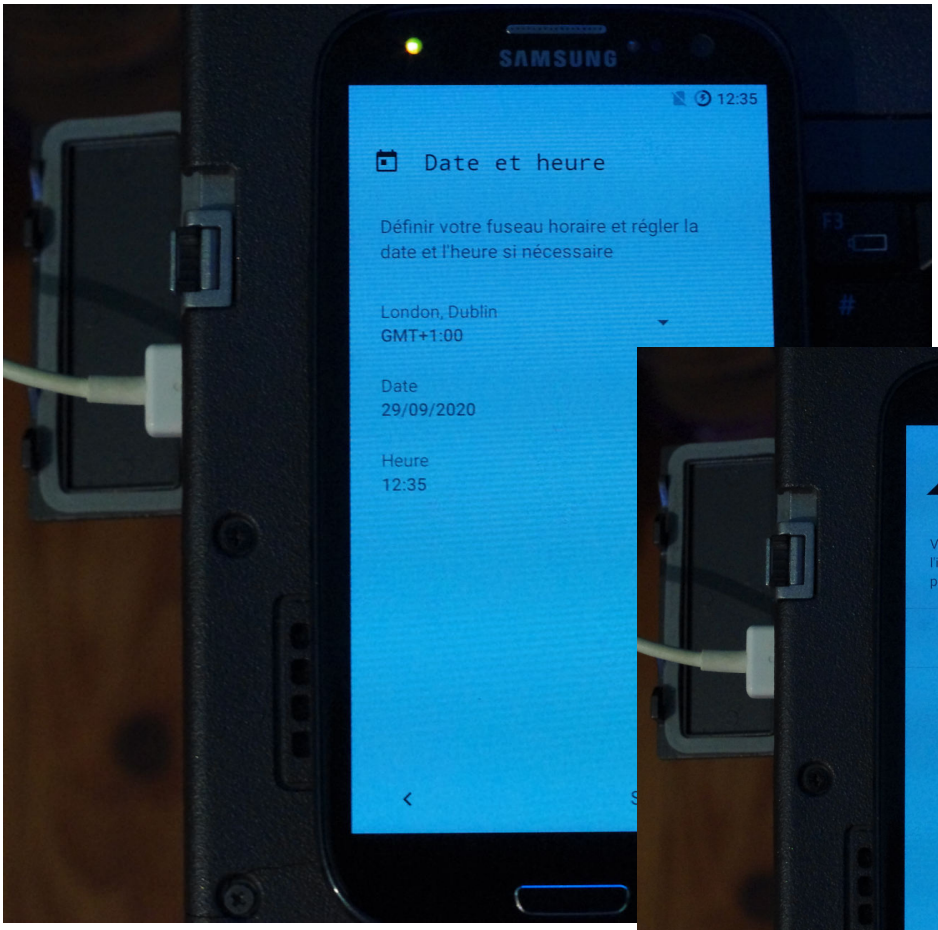
Par la suite on pourra changer tout ça. Il ne s'agit que de la langue par défaut; bien sûr c'est bien de mettre sa langue (à moins qu'on veuille se forcer à apprendre une autre langue!)

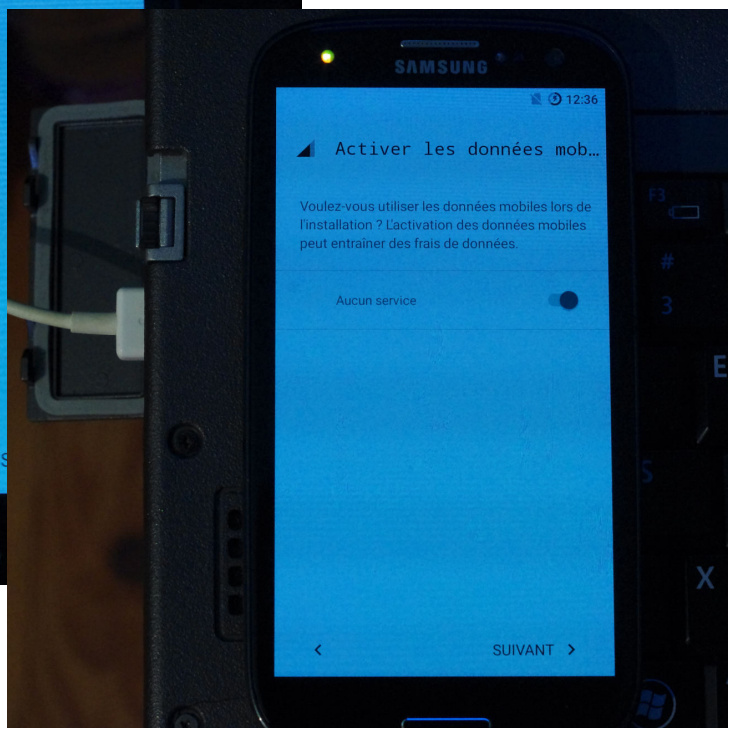
On appuie sur "Suivant"




On choisit le fuseau horaire, et le format d'affichage de l'heure.

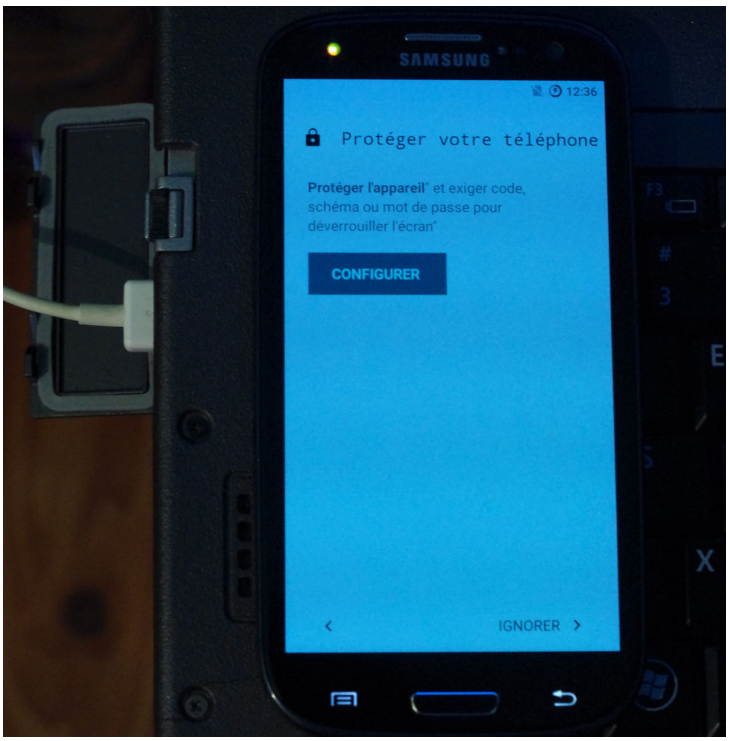
Je préfère par précaution mettre l'heure de là où je me trouve le plus souvent, parce que l'heure est liée à des processus système (mises à jour, etc...)




Après avoir appuyé sur "Suivant" pour la date et l'heure, on arrive à l'écran d'activation des données mobiles (comme la 3G par exemple).

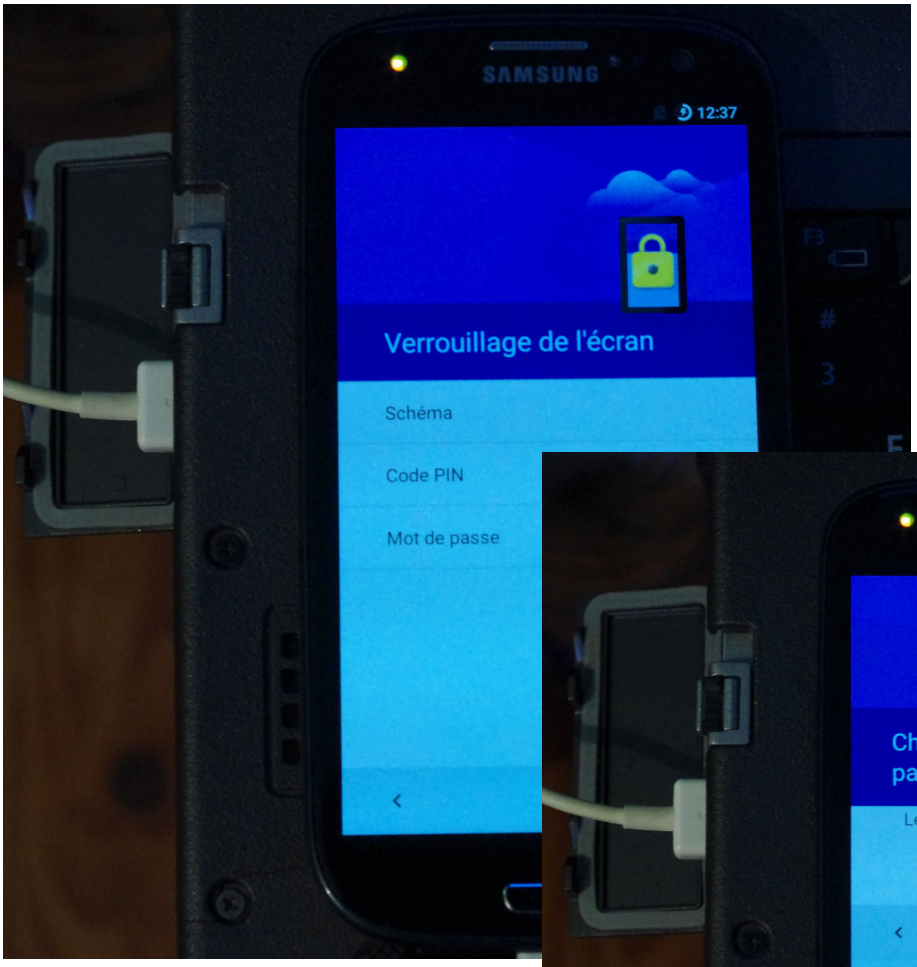
Par prudence pour celles et ceux qui ont des petits forfaits, il vaut mieux ne pas l'activer, ça ne sera pas absolument nécessaire ici pour l'instant (il faudra plafonner les données mobiles par la suite (voir tuto sur la post-installation).




On arrive au stade du mot de passe de déverrouillage d'écran.

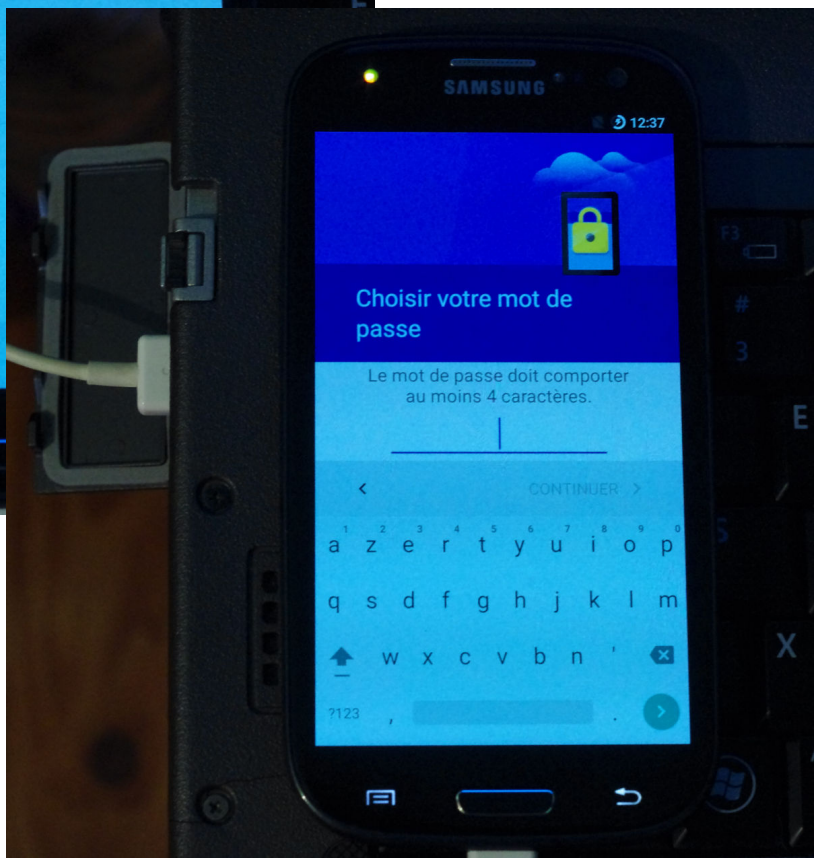
Je préfère mettre un mot de passe texte assez pénible et peu pratique, et changer par la suite en utilisant un schéma (pas trop simple quand même, mais plus utilisable quand on veut déverrouiller l'écran rapidement).

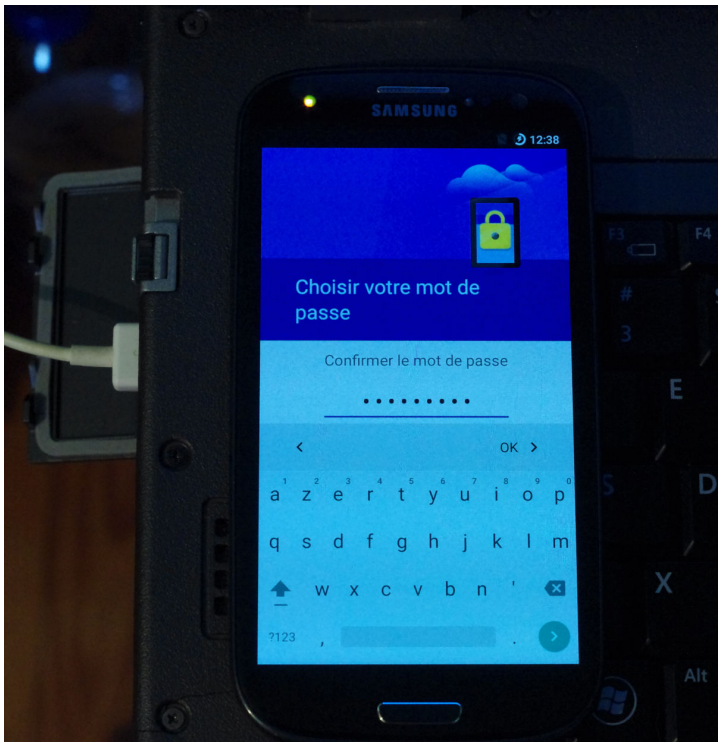
Il y a des options pour déverouiller plus rapidement et que pour l'appareil photo.



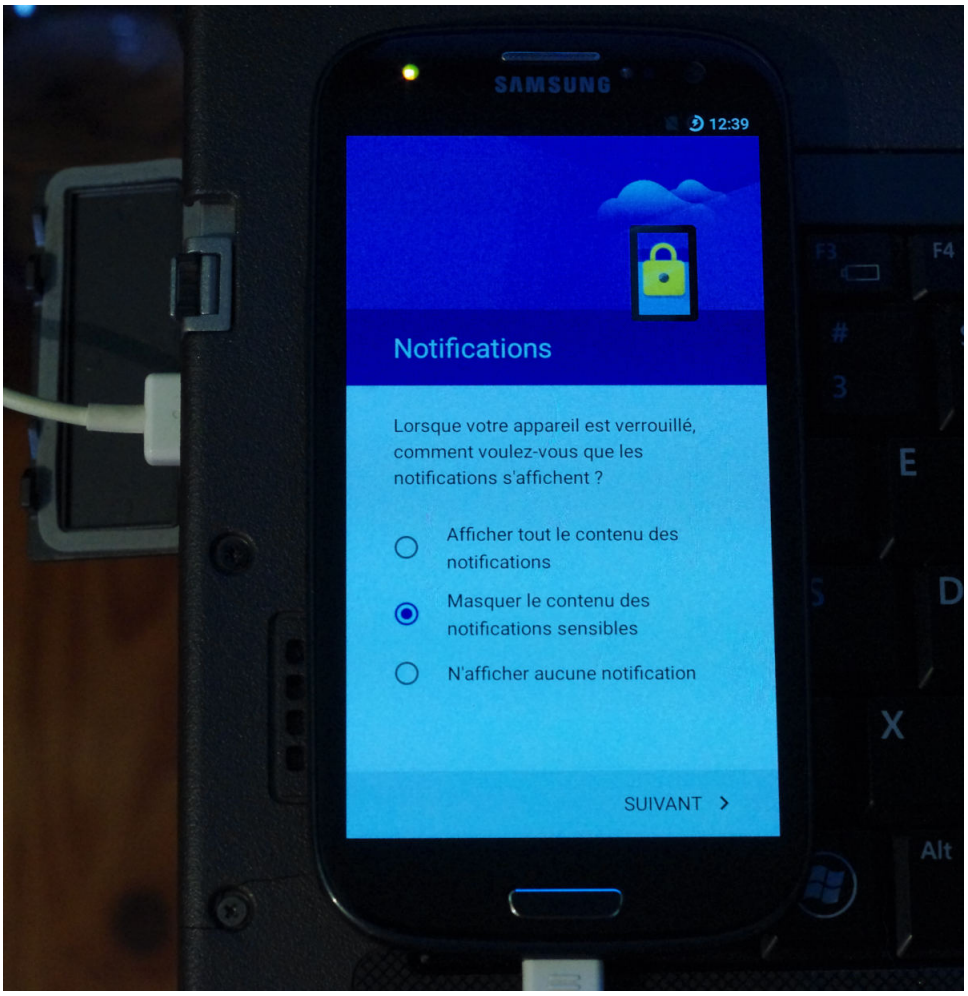

Je choisis donc "Mot de passe".

Puis je le tape une première fois. Par sécurité il va demander une confirmation.



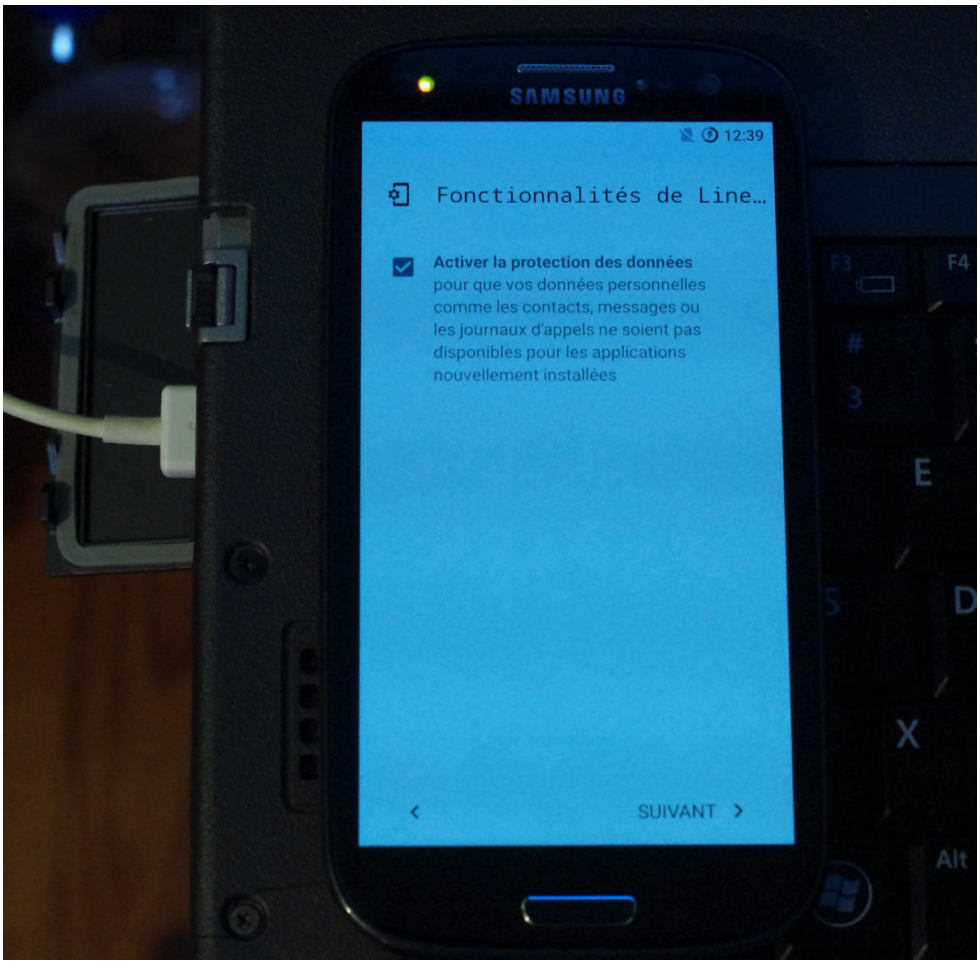




Puis je fais "Ok".




Ce menu permet de choisir si on veut que les notifications (sms reçus, mails, messages, et autres) apparaîssent avec les détails quand l'écran est verrouillé, ou non.

Je choisis "Masquer le contenu des notifications sensibles" pour avoir une idée de quel programme a "vécu" un évènement mais sans les détails.

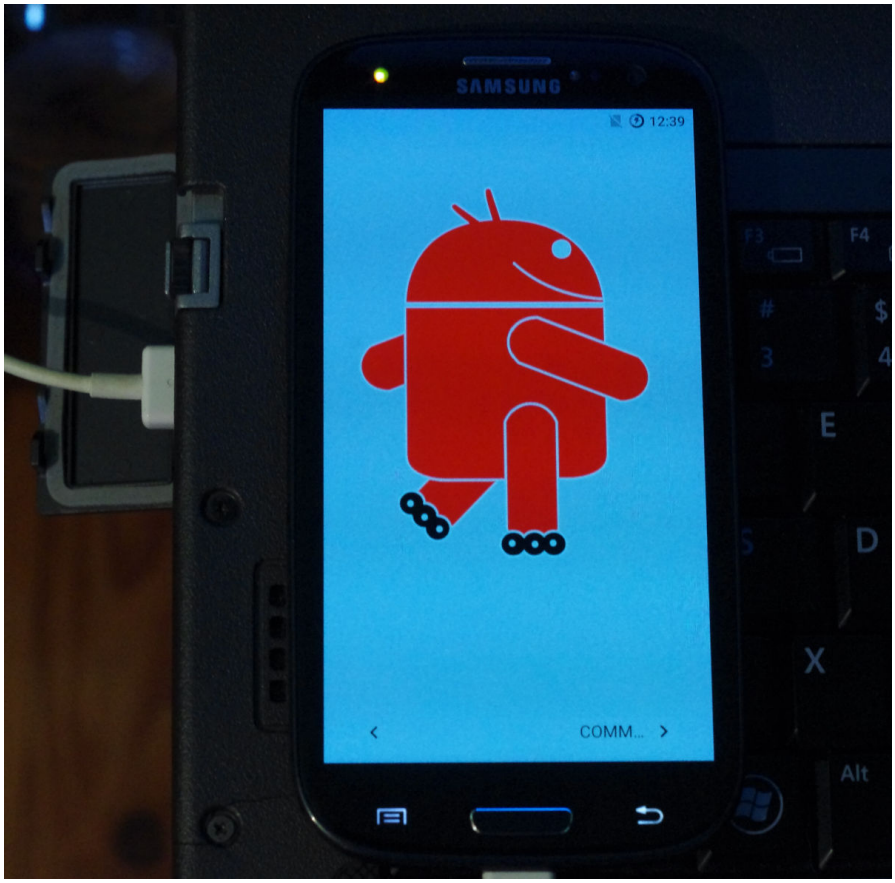



Bien penser à activer cette fonction, qui est importante.

Les programmes nouvellement installés peuvent être demandeurs de trop d'informations, ou simplement on ne veut pas leur donner certaines informations.
Dans le cas de replicant il ne faut jamais donner la possibilité à un programme d'avoir la localisation: parce que le GPS ne fonctionne pas (il n'y a pas actuellement les pilotes libres pour le faire tourner) et donc le programme peut planter.

En règle générale il est plus prudent d'autoriser les programmes à accéder aux données par la suite mais pas tout de suite à l'installation.

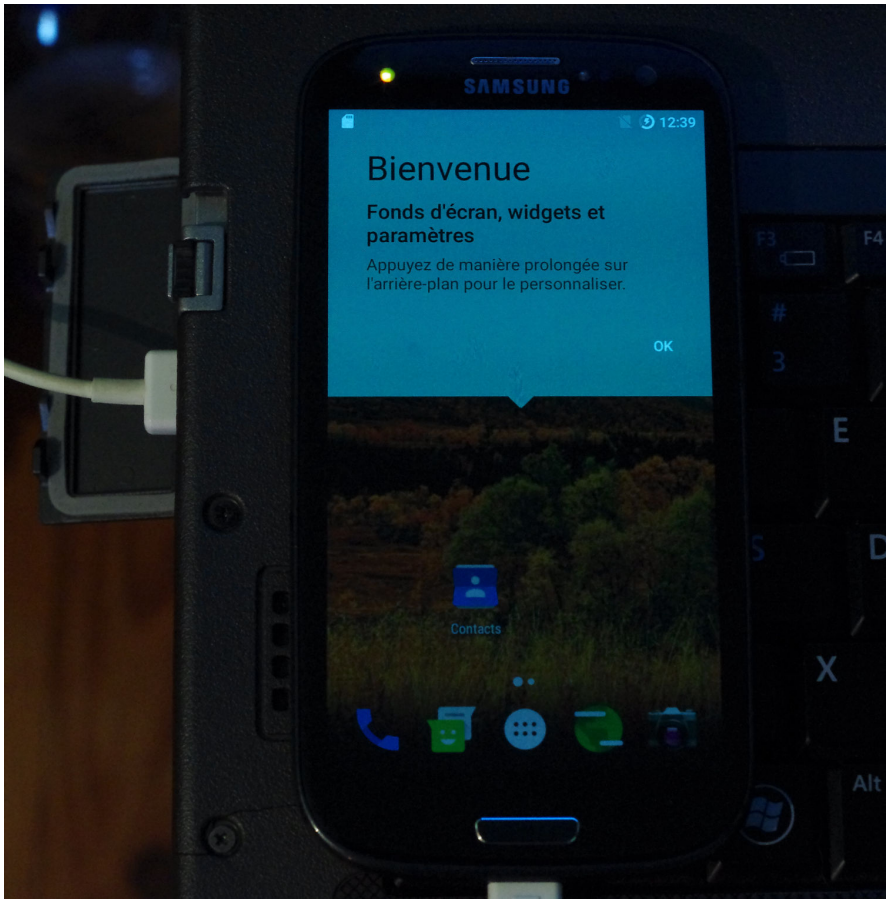
L'installateur de programmes et gestionnaire de mises à jour de replicant est f-droid. Les personnes qui sont derrière contrôlent et font attention aux programmes proposés, mais on n'est jamais à l'abri d'une erreur, d'un bug, ou d'une personne malveillante ayant mis en ligne une fausse version mobile d'un programme connu.




On arrive à la fin des réglages de premier démarrage.

On va arriver à l'interface graphique de replicant.

Tout en haut on voit déjà l'heure, l'état de la batterie, et le réseau (comme j'ai pris une version non conseillée de replicant et pas la 003 je n'ai pas de réseau et il ne détecte pas la carte SIM.




On arrive à l'interface graphique.

Il y a encore pas mal de réglages à faire, et des programmes à installer. C'est pour cela qu'il y a le deuxième tuto sur la post-installation.

Les icônes qu'on voit sont des raccourcis de programmes couramment utilisés. Le rond blanc avec les petits points dedans est le menu avec tous les programmes disponibles. N'hésitez pas à cliquer un peu partout et à glisser les doigts dans toutes les directions pour trouver des menus cachés.

Quand on glisse le doigt du haut de l'écran vers le bas apparaît un menu avec les notifications, puis quand on continue à glisser apparaît un menu avec des fonctions comme la luminosité de l'écran, le mode avion, etc...

Quand on glisse le doigt d'un des bords latéraux de l'écran en s'en éloignant on arrive à la suite de la photo de la forêt automnale, et à d'autres icônes de raccourci.

On arrive à la fin de ce tutoriel.
Le téléphone obtenu est totalement indépendant de Google, permet d'avoir plus de sécurité, un système plus léger, et quelques fonctions bien sympathiques.

Ce n'est pas non plus miraculeux et totalement sûr; par exemple certains programmes de sécurité comme Snoopsnitch ne sont pas compatibles, les gens de replicant manquent de moyens et de personnes pour les aider à améliorer encore tout ça.

On peut chiffrer toute la mémoire du téléphone, ce qui est bien intéressant.

Les développeurs de replicant ont créé Repwifi pour pouvoir avoir une connexion wifi fonctionnelle avec une clé wifi compatible (thinkpenguin par exemple).

La vidéo, la 3D, le GPS, le wifi sans clé wifi externe, le bluetooth, le panoramique, l'appareil photo face écran ne marchent pas faute de pilotes libres. Les personnes responsables de replicant ont préféré ne pas faire fonctionner tout ça plutôt que de risquer de compromettre le téléphone.

Si vous avez des questions, vous pouvez nous contacter avec le mail cnnr-numerique@riseup.net

Fait dans le cadre du groupe de travail du CNNR sur le numérique éthique