

### نبذة عن النظام :

تاييلز هو نظام تشغيل حر مفتوح المصدر مبني على دبيان جنو / لينكس يهدف إلى الحفاظ على خصوصية وأمان المستخدمين على شبكة الإنترنت، يساعدك نظام تاييلز في استخدام الإنترنت بخفاء وبعيداً عن الرقابة الإلكترونية من قبل مزودي الخدمة أو الحكومات، يمكنك استخدام نظام تاييلز على معظم أجهزة الكمبيوتر حيث لا يتطلب إمكانيات عالية لتشغيله ولا يترك أي أثر على جهاز الكمبيوتر.



**نظام تاييلز**

**TAILS OS**



الحمد لله معز الإسلام بنصره ومذل الشرك بقهره ومصرف الأمور بأمره ومستدرج الكافرين بمكره الذي قدر الأيام دولاً بعدله وجعل العافية للمتقين بفضله والصلة والسلام على من أعلى الله منار الإسلام بسيفه وعلى آله وصحبه ومن تبعهم يا حسان إلى يوم الدين

### تايلز

**تايلز** هو نظام تشغيل حر مفتوح المصدر مبني على ديبيان جنو / لينكس يهدف إلى الحفاظ على خصوصية وأمان المستخدمين على شبكة الإنترنت، يساعدك نظام **تايلز** في استخدام الإنترنت بتخفٍ وبعيداً عن الرقابة الإلكترونية من قبل مزودي الخدمة أو الحكومات، يمكنك استخدام نظام **تايلز** على معظم أجهزة الحواسيب حيث لا يتطلب إمكانيات عالية لتشغيله ولا يترك أي أثر على جهاز الكمبيوتر.

#### ١. استخدام شبكة الإنترنت بتخفٍ والتغلب على الحجب من خلال شبكة تور :

تور شبكة تخفٍ مفتوحة المصدر تحمي خصوصيتك على الإنترنت وتتمرر إتصالك عبر شبكة من الخوادم موزعة عبر العالم ويديرها متطوعون، تمنع شبكة تور مزودي الخدمة والحكومات من معرفة المواقع التي تزورونها وتمنع هذه المواقع من تحديد أماكن تواجدكم

نظام **تايلز** يجبر كافة الإتصالات بالإنترنت على المرور من خلال شبكة تور وإذا حاول أحد البرامج الإتصال بشبكة الإنترنت مباشرة وليس من خلال تور يتم حظره تلقائياً.

#### ٢. عدم ترك أي أثر على جهاز المستخدم :

تم إعداد **تايلز** بحرص للاستغناء عن القرص الصلب (Disk Hard ) ويعتمد نظام **تايلز** على ذاكرة الوصول العشوائي (RAM) في الحاسوب والتي يتم محوها تماماً بعد بضع ثوان أو دقائق عند إعادة تشغيل الجهاز لهذا قد تتمكن قوات مداهمة إذا كانت تتبع المستعمل من تجميد ذاكرة الوصول العشوائي حرفيأً (RAM) ثم إستخراج معلومات داخلها لاحقاً -كون التجميد يمنع حفظ RAM- و الحل الوحيد لمثل هذه الحالات هو استعمال التوزيعة في مكان آمن.

**تايلز** لا يؤثر على النظام الرئيسيالمثبت على الحاسوب ولا يعدل عليه بأي شكل من الأشكال، إذا يمكنك استعمال **تايلز** على أي جهاز سواء كان جهازك الخاص أو جهاز صديقك أو أي أجهزة أخرى وبعد فصل الـ **USB** لن يبقى أي أثر لاستخدام **تايلز** ويمكنك إعادة تشغيل الحاسوب على نظامه المعتمد



## ٢. استخدام أدوات التشفير للملفات الخاصة والبريد الإلكتروني :

يحتوي نظام **تايلز** على العديد من البرامج المهمة مسبقاً لحفظ على خصوصية وأمان المستخدمين من بينها متصفح الإنترنت، برنامج البريد الإلكتروني، برامج مكتبة، محرر صور ، محرر صوتيات إلخ... يحتوي أيضاً على مجموعة مختارة من أدوات حماية البيانات الخاصة التي تستخدم التشفير مثل :

- تشفير جهاز تخزين **USB** أو قرص ثابت خارجي باستخدام نظام تشفير لينكس **LUKS**.
- التبديل التلقائي إلى بروتوكول **HTTPS Everywhere** عند تصفح موقع تدعم استعمال " **HTTPS Everywhere**" وهذه إضافة لمتصفح فايرفوكس طورتها مؤسسة الحدود الإلكترونية EFF.
- تشفير وتوقيع البريد الإلكتروني من خلال بروتوكول **PGP** وتشفي رسانكم ببروتوكول **OTR** و **OMEMO**.
- حماية محادثات رسانكم الفورية باستخدام أداة **Pidgin** وتشفي رسانكم ببروتوكول **OTR** و **OMEMO**.
- محو الملفات وتنظيف مساحة القرص في جهازكم باستخدام إضافة **Nautilus Wipe**
- لوحة مفاتيح إفتراضية (**Florence**) تمكن من إدخال كلمات المرور من خلال النقر على الماوس بدلاً من الاضطرار للكتابة على لوحة المفاتيح للحماية من الكي لوجر الذي يقوم بتسجيل كل الأشياء التي تتم كتابتها على لوحة المفاتيح.
- حذف البيانات الوصفية الموجودة في الملفات كالصور والمستندات من خلال أداة **MAT**

## المرحلة الأولى : التحميل والتحديث

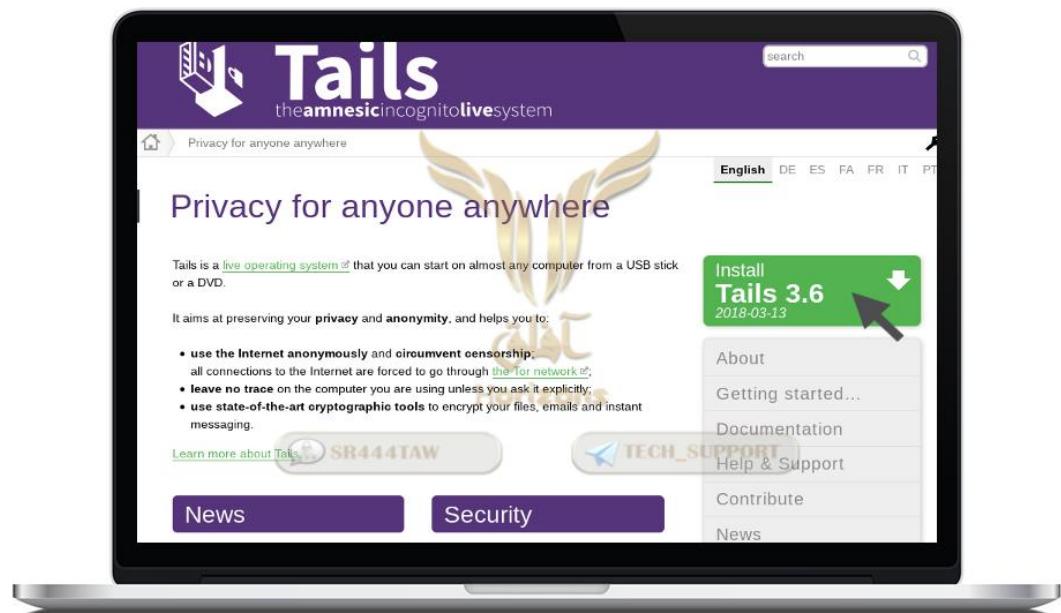
### أولاً : تحميل توزيعة تايلز من الموقع الرسمي

- ◎ توجه إلى الموقع الرسمي لنظام **تايلز** من خلال متصفح فايرفوكس مع VPN أو متصفح تور [رابط الموقع](#)

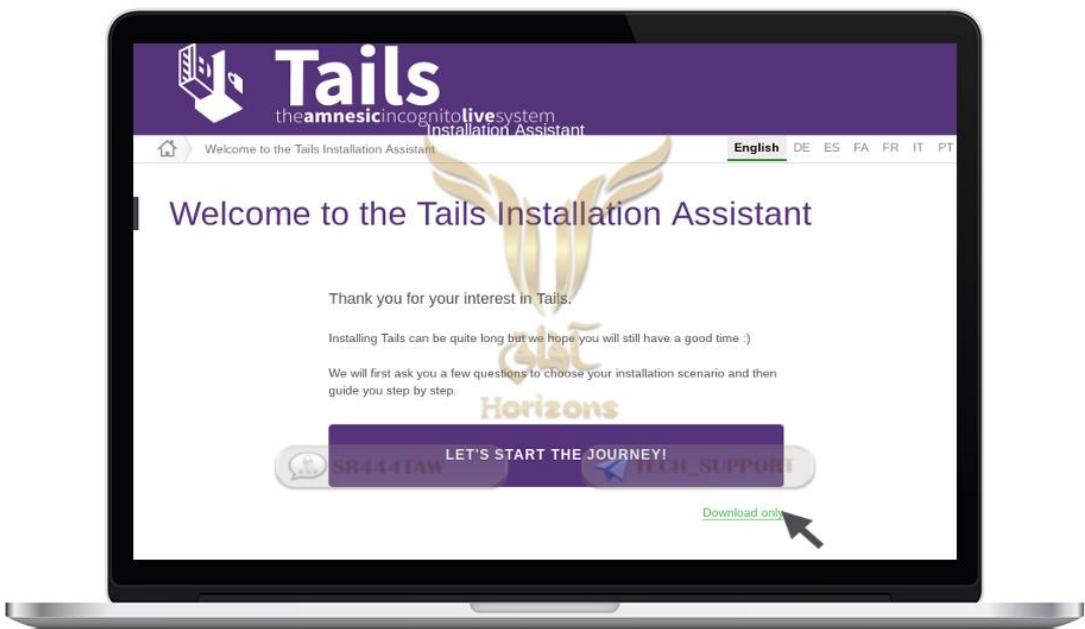
**ملاحظة :** احرص على استخدام شبكة تور أو خدمات الـVPN أثناء تحميل توزيعة Tails لأن مزود الخدمة **يستطيع معرفة المواقع التي تتصفحها في حال لم تستخدم تور أو VPN**

- ◎ لبدء عملية التحميل اضغط على **Install Tails**





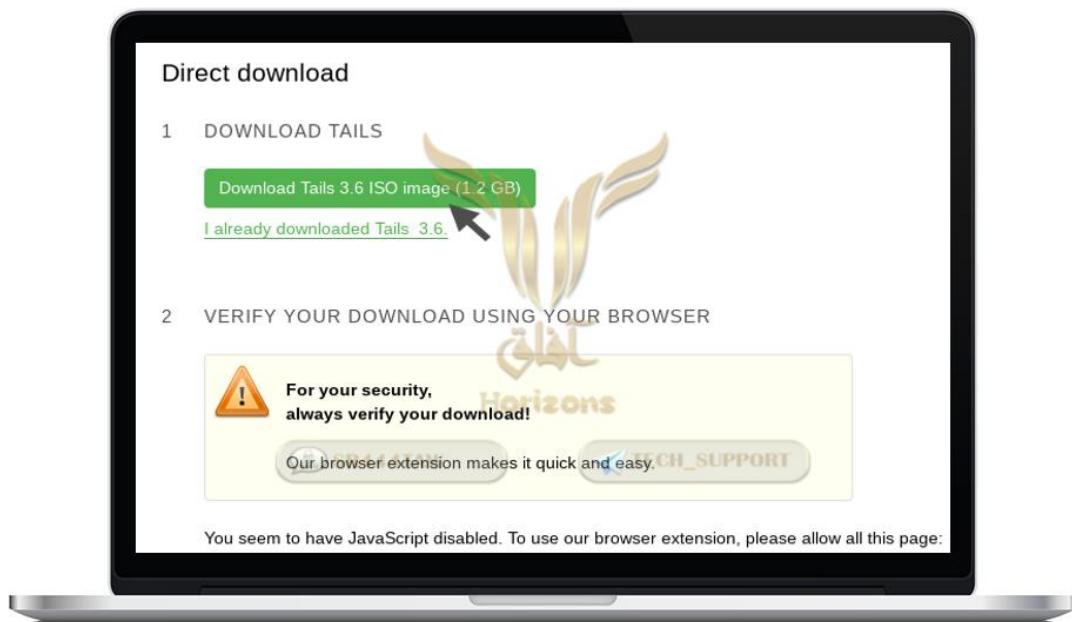
**Download Only** ↗



< ستجد خيارات ↗

- التحميل المباشر ( Direct Download ) :

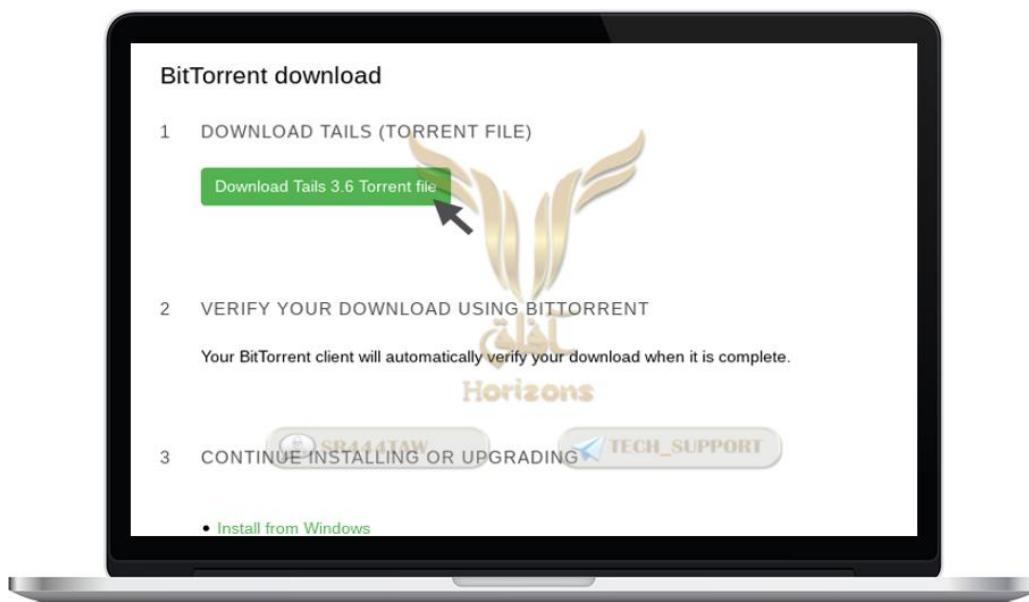




### - التحميل عن طريق شبكة تورنت ( BitTorrent download )

شرح تحميل الملفات عبر شبكة تورنت بأمان من [هذا](#)

**ملاحظة :** تحقق من تحديث البرنامج المستخدم في التحميل لتجنب الثغرات الأمنية.

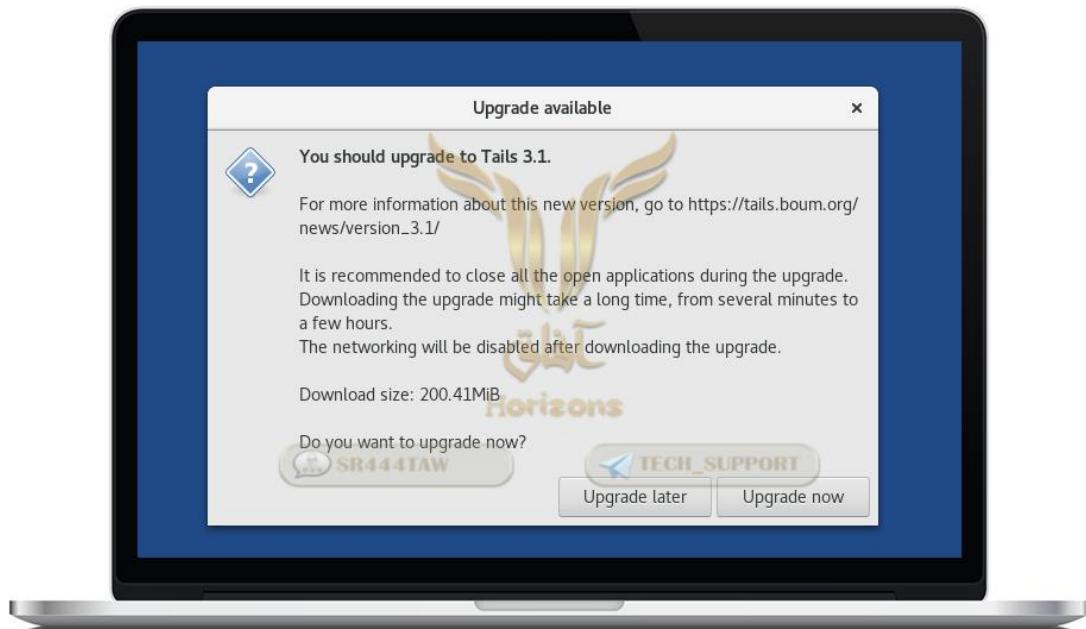


ثانياً : تحديث توزيعة تايلز



يقوم مشروع تور بإصدار نسخة جديدة كل شهر من توزيعة تايلز حيث تحتوى النسخة الجديدة على تحديثات أمنية لغلق الثغرات والأخطاء الموجودة بالنسخ السابقة إذا عملية التحديث ضرورية جداً لمستخدمي نظام تايلز فمن المحتمل أن يخترق جهازك أو يتم تعقبك إذا كنت تستخدم نسخة غير محدثة من نظام تايلز فاحرص دائماً على تحديث النظام.

- توزيعة تايلز تتحقق من وجود **تحديثات فرعية** للنسخة التي حملتها مسبقاً بشكل تلقائي عند الإتصال بشبكة الإنترنت أثناء مرحلة تشغيل النظام حيث أن تحديث توزيعة تايلز يوفر على المستخدم تحميل التوزيعة بالكامل من الموقع الرسمي بالإضافة إلى أن توزيعة تايلز تتحقق تلقائياً من البصمة الرقمية للنسخة الجديدة عند إستلامها.



## || المرحلة الثانية : التحقق من البصمة الرقمية (إختيارية) ||

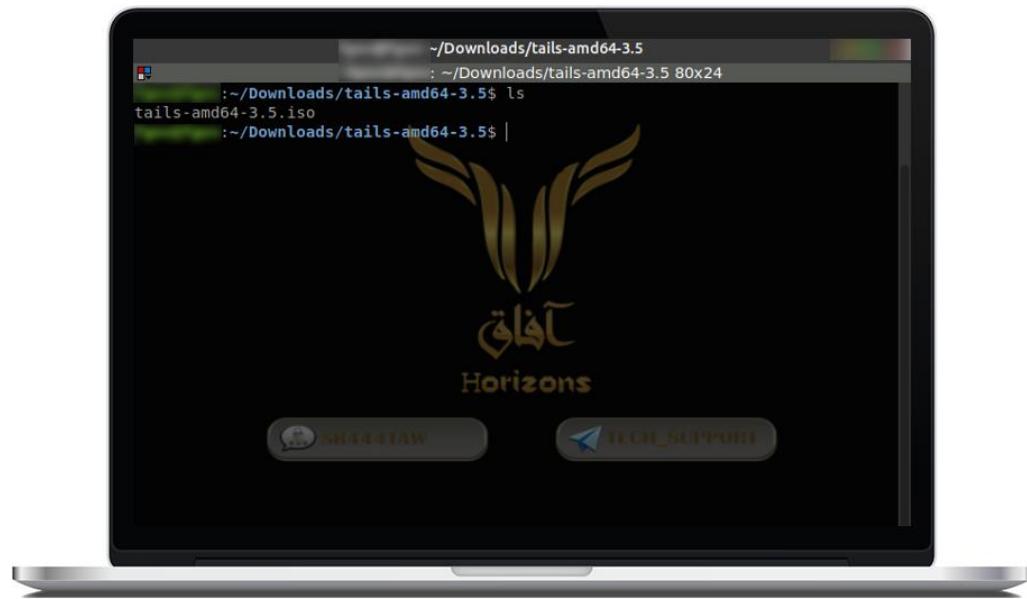
### ال بصمة الرقمية :

هي علامة أمان إلكترونية تعتمد على علم التشفير في إنشاء توقيع رقمي للملفات حيث يمكن إضافة التوقيع إلى الملفات أو التطبيقات مما يتيح لك إمكانية التحقق من ناشر الملف كما تساعد في التتحقق من أن الملف لم يتم تغييره منذ تم توقيعه رقمياً أو التعديل عليه (إذا تستطيع معرفة إذا ما كان الملف أو التطبيق تم التعديل عليه أم لا من خلال البصمة الرقمية)

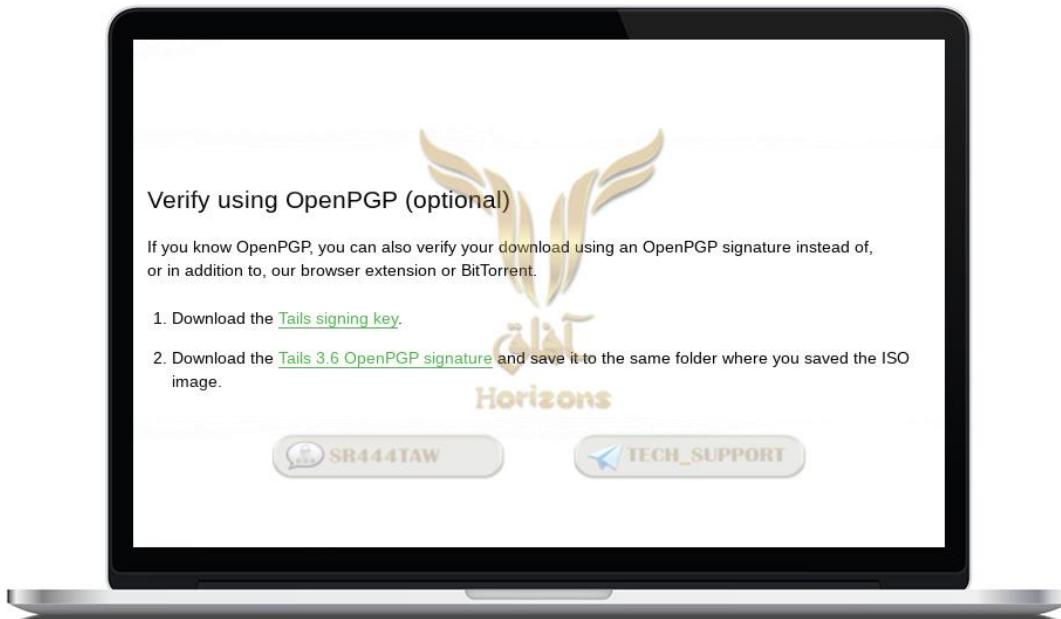
- للتحقق من سلامة ملف توزيعة تايلز يجب التتحقق من البصمة الرقمية لتوقيع المطور عن طريق بروتوكول **OpenPGP**

**أولاً : التتحقق من البصمة الرقمية لمستخدمي لينكس :**

- افتح سطر الأوامر أو الطرفية (Terminal) في مجلد تحميل التوزيعة



- حمل Tails 3.x OpenPGP signature و Tails signing key من [الموقع الرسمي](#)

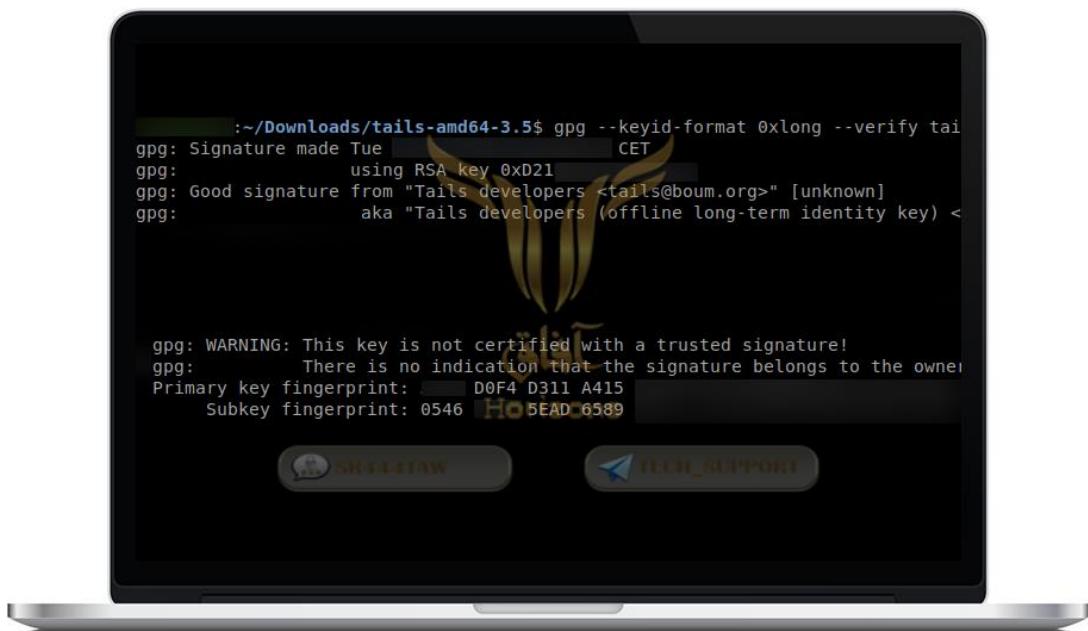


بعد التحميل اكتب الأمر التالي على سطر الأوامر أو الطرفية و احرص على وجود ملف التوزيعة بنفس مسار مفتاح OpenPGP الذي قمت بتحميلها مؤخراً

```
tails-amd64-3.6.iso.sig tails-amd64-3.6.iso gpg --keyid-format 0xlong --verify
```

**ملاحظة :** احرص على تغيير أسماء الملفات حسب إصدار النسخة التي قمت بتحميلها

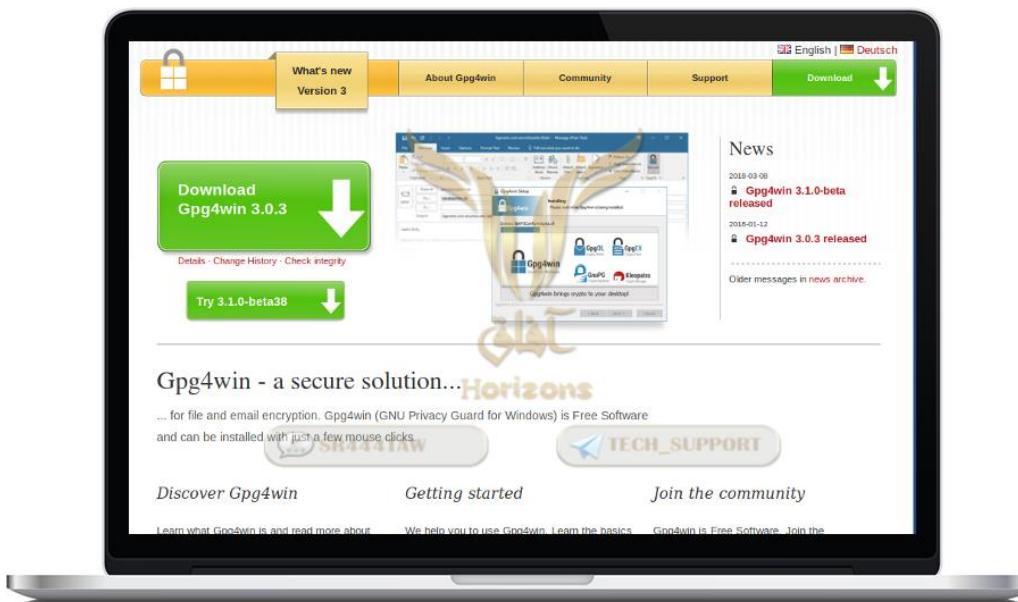
◎ النتيجة :



- إذا كانت النتيجة تحتوي **Good signature** فنسخة التوزيعة آمنة من التعديل.

- إذا كانت النتيجة تحتوي **WARNING** فنسخة التوزيعة ليست آمنة وقد تعرضت للتعديل.

- ثانياً التحقق من البصمة الرقمية لمستخدمي ويندوز :  
◎ توجه إلى موقع [Gpg4Win](#) و اضغط **Download**



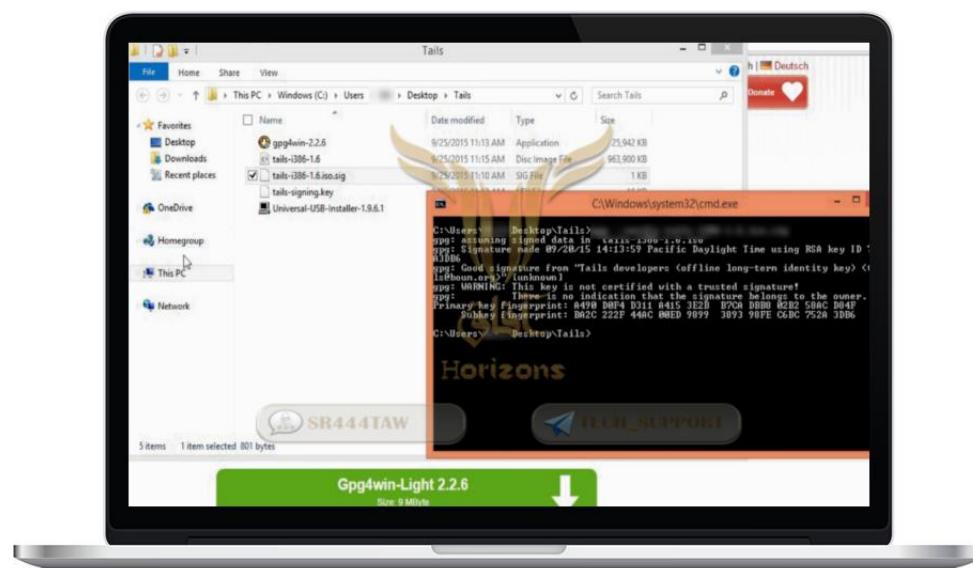
#### • بعد التحميل ثبت البرنامج...

ثم افتح موجه الأوامر CMD بمسار التحميل حيث تتوارد الملفات : **tails-signing.key** ، **tails-xx.iso** ، **tails-xx.iso.sig**

(و التي تطرقنا لتحميلها سابقاً من الموقع الرسمي)

#### • نضع الأمر السابق :

**tails-amd64-3.6.iso.sig tails-amd64-3.6.iso gpg --keyid-format 0xlong --verify**



(و هنا ظهرت نتيجة إيجابية و سلبية في نفس الوقت فلا نبالي بالأختير)

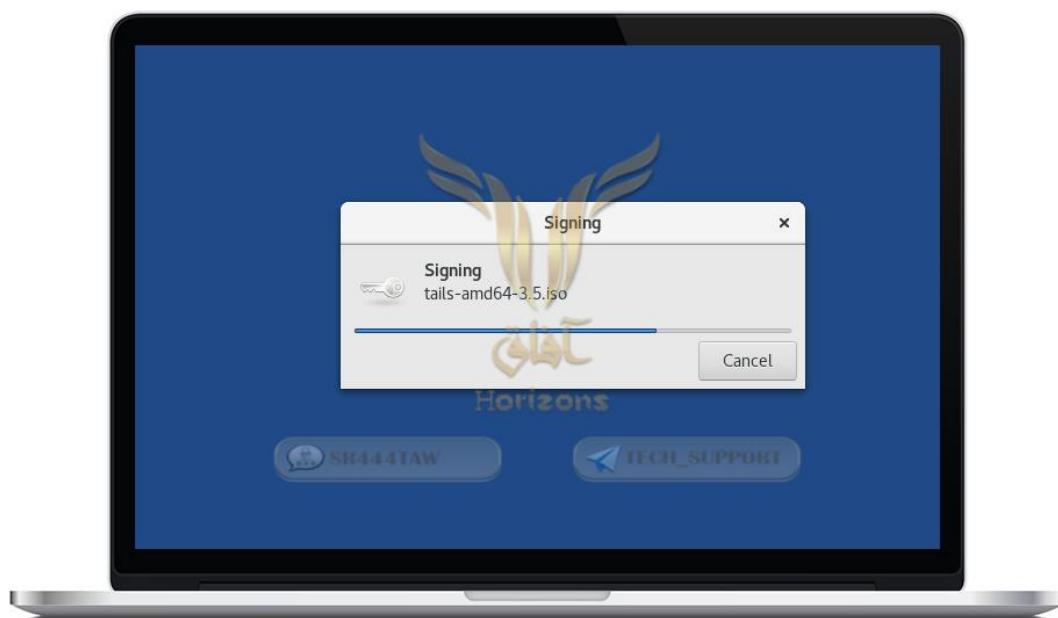


- التحقق من داخل نسخة **Tails** :

(نشرح كيفية الإقلاع لاحقاً)

- توجه إلى مسار تحميل التوزيعة للهارد ديسك أو مفتاح USB حيث تتوارد نسخة توزيعة **Tails** بأمتداد .iso.

- نضغط يمين بالماوس على نسخة التوزيعة ونختار **Open With Verify Signature**



- بعدها سيأتي إشعار فيه هل النسخة متلاعب بها أو لا.

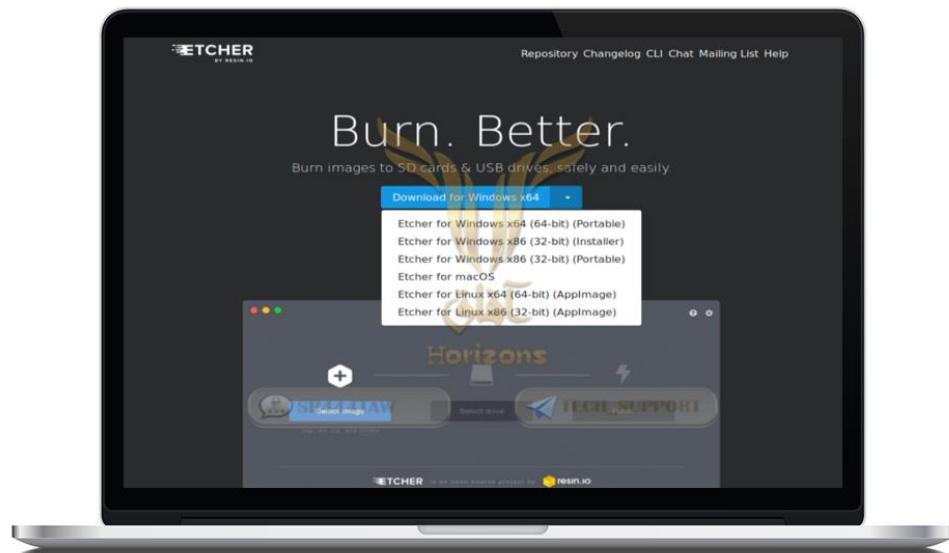


- هنا وجدنا النسخة سليمة **Good Signature**

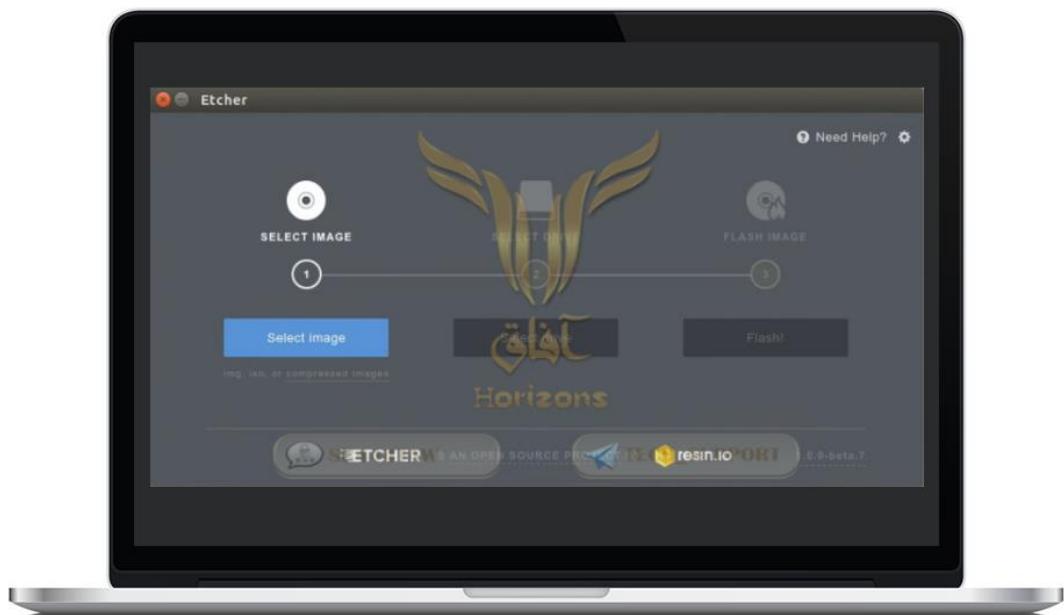
## المرحلة الثالثة : الحرق و الإقلاع

### حرق توزيعة تايلز

- توجه إلى الموقع الرسمي لبرنامج **Etcher** و حمل نسخة البرنامج حسب النظام الذي تستخدمه:



- قم بتوصيل ال **USB** بالحاسوب وتتابع الخطوات الموضحة في الشرح لينكس و ويندوز : [من هنا](#)



## ثانياً : الإقلاع

- نبقي مفتاح USB بالجهاز و نعيد تشغيله ثم نكرر الضغط على F12 و ستظهر لك قائمة الإقلاع اختار منها:

**USB Disk ثم Removable USB**



- إذا لم ي عمل مفتاح F12 معك فلكل مصنع حواسيب زر معين لإظهار قائمة الإقلاع ذكر منهم:

**F12 – Acer**



F8 – ASUS

F12 – Dell

F9 – HP

F12 – Lenovo

F2 – Samsung

F11 – Sony

F12 – Toshiba

• للإطلاع على بقية إعدادات بقية المصنعين [اضغط هنا](#)

- لأصحاب الحواسيب المكتبية المركبة أبحث عن إعدادات مصنع (اللوحة الأم) MotherBoard

- إذا واجهتك مشكلة في الإقلاع من USB شاهد هذا [الشرح](#) أو يمكنك التواصل معنا عبر حسابات الدعم الفنى- و سنقدم العون بإذن الله.

## || المرحلة الرابعة : شرح واجهة النظام ||

• شرح واجهة البداية:

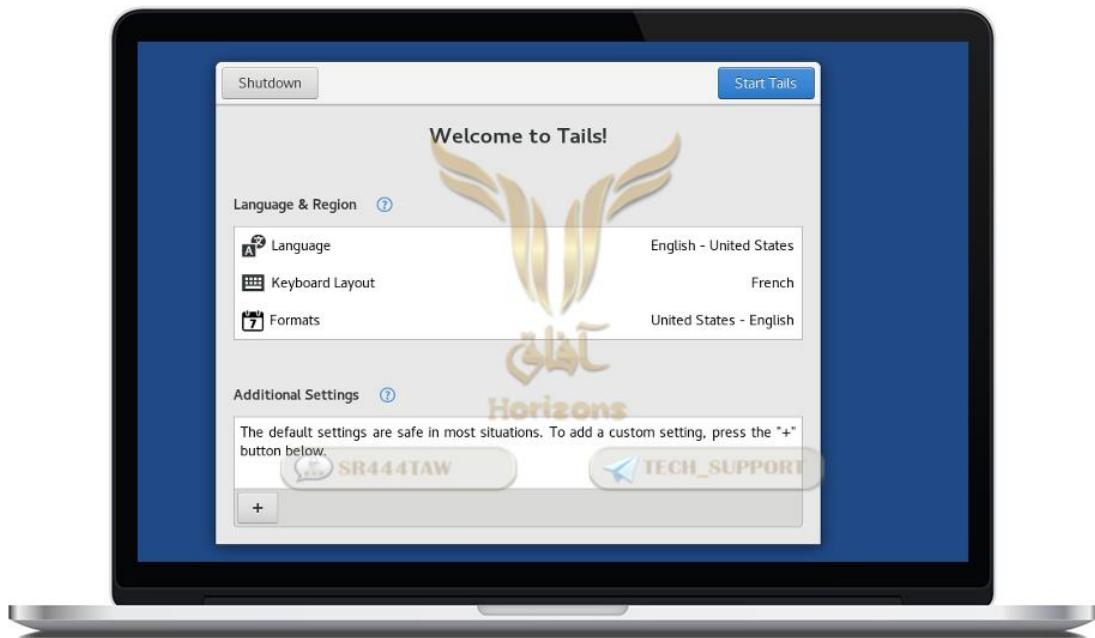
- الخانة الأولى Language : ضع لغة النظام العامة

(نصح بالإنجليزية حتى إذا واجهتك مشكلة لا قدر الله يسهل إيجاد الحل على الإنترنت)

- الخانة الثانية Keyboard Layout : إختر لغة لوحة المفاتيح (هنا وضعنا الفرنسية)

- الخانة الثالثة Formats : ضبط إعدادات التوقيت بالتوقيت (لا داعي للتغييرها)





• نضغط على علامة + أسفل يسار النافذة



• نجد خيارات أخرى :

- نضغط على الأولى **Administration Password** لاختيار كلمة سر لمدير النظام (قم بتعيين كلمة مرور للنظام يفضل أن تكون كلمة مرور قوية تتكون من حروف وأرقام ورموز وأطول من ٢٠ عنصر)

- ثم الأخيرة **Configure a Tor Bridge or local proxy** و نغيرها إلى **Network Connection** ثم **Add** نضغط



• ثم نضغط Start Tails

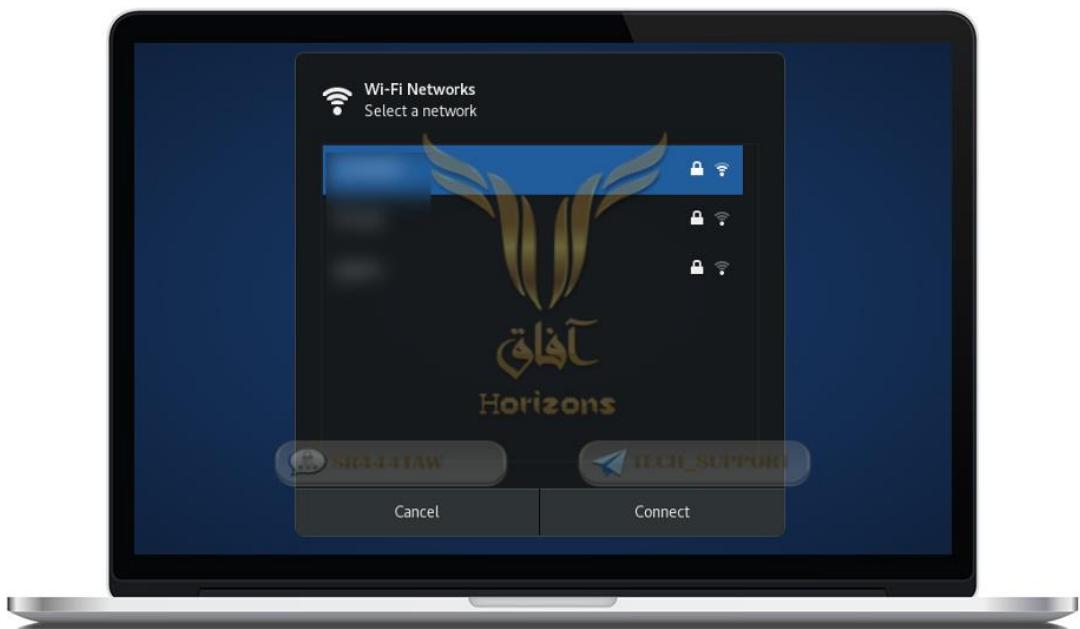


• الآن علينا ضبط الإتصال بالشبكة، نضغط على الأيقونة أعلى يمين الشاشة

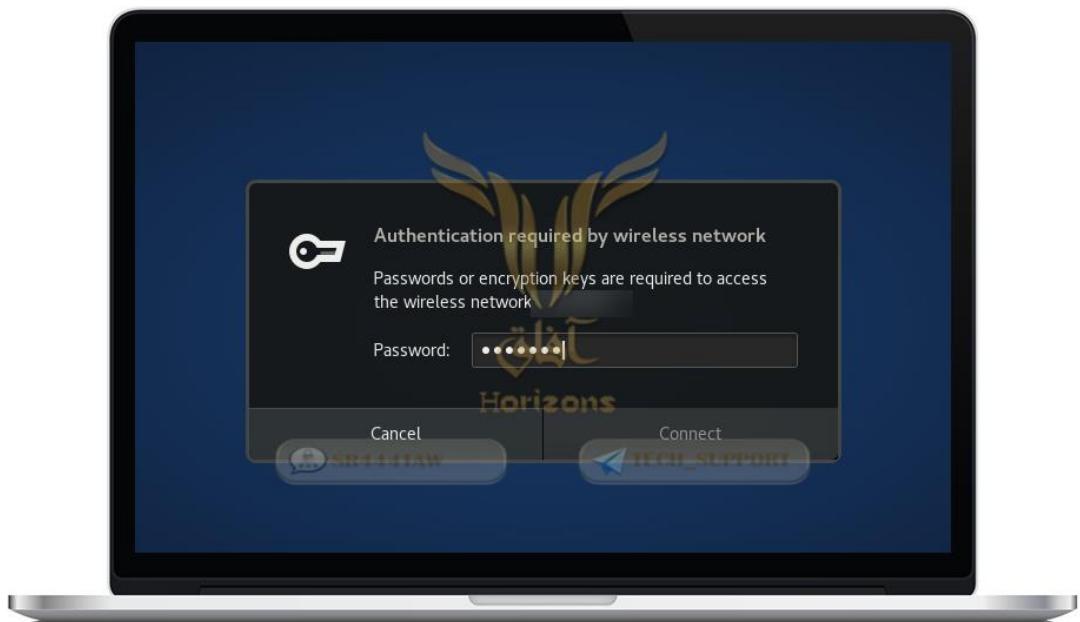


• نختار الشبكة التي نريد الإتصال بها





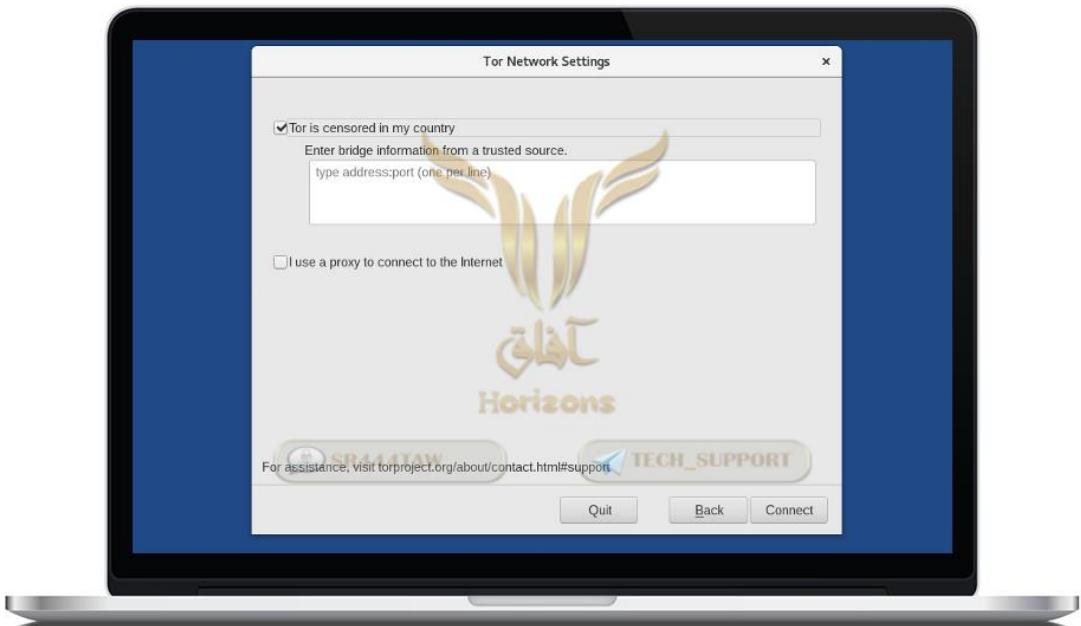
• ثم ندخل كلمة السر



● بعد الاتصال بالشبكة تظهر لنا نافذة للاتصال بالتور



### • نختار **Tor is Censored in My country** ثم **Configure**



- لا ننصح بالإتصال بشبكة التور مباشرة لترجينا أن المتصلين مباشره يتم مراقبتهم لهذا نستعمل الجسور و نضعها في الخانة السابقة، تحصل على الجسور من [هنا](#)

- إذا لم يتوفر لديك جهاز آخر لسحب الجسور بإمكانك استعمال المتصفح الغير أمن (**Unsafe Browser**) للدخول للموقع و استخراج الجسور.

**Unsafe Browser < Internet < Applications**



و هناك طريقة أخرى لسحب الجسور بدون الدخول للموقع مباشرة :

- عن طريق المتصفح الغير الآمن ندخل لحساب **Riseup** أو **gmail** أو **yahoo** - التسجيل مغلق حالياً في الأخير .

- نقوم بإرسال رسالة فارغة للبريد [bridges@torproject.org](mailto:bridges@torproject.org)

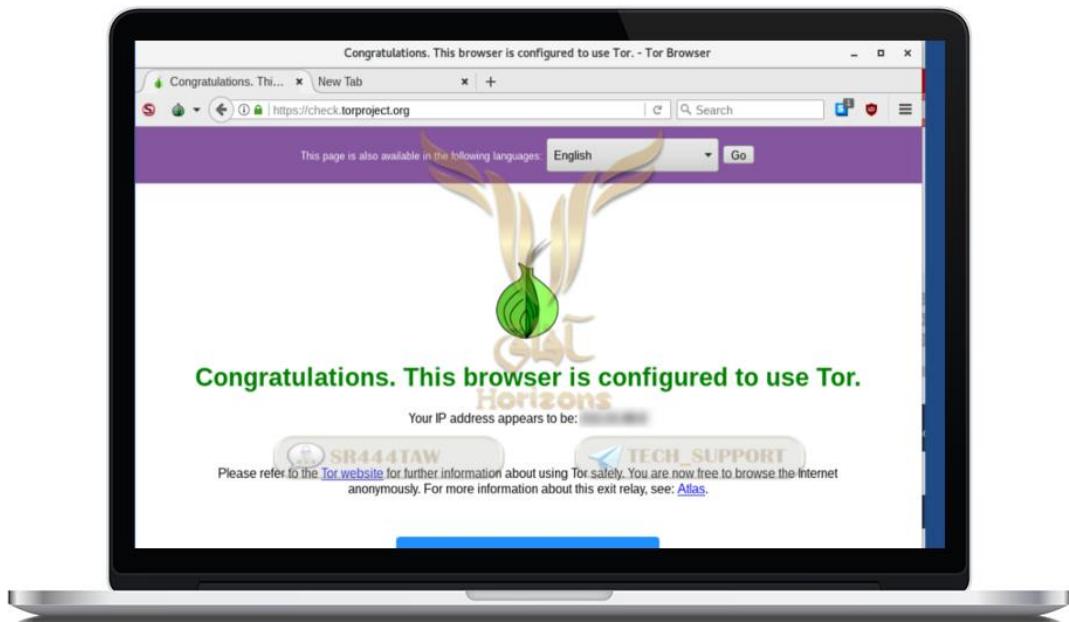
ثم نستقبل رسالة فيها الجسور التي تستعملها (هذه الطريقة لا تعمل دأماً)

- بعد تحصيل الجسور نضعها في الخانة السابقة ثم نضغط **Connect**



بعد الدخول لمتصفح التور نتوجه للموقع حتى نتحقق أن إتصالنا بشبكة التور ليس وهماً

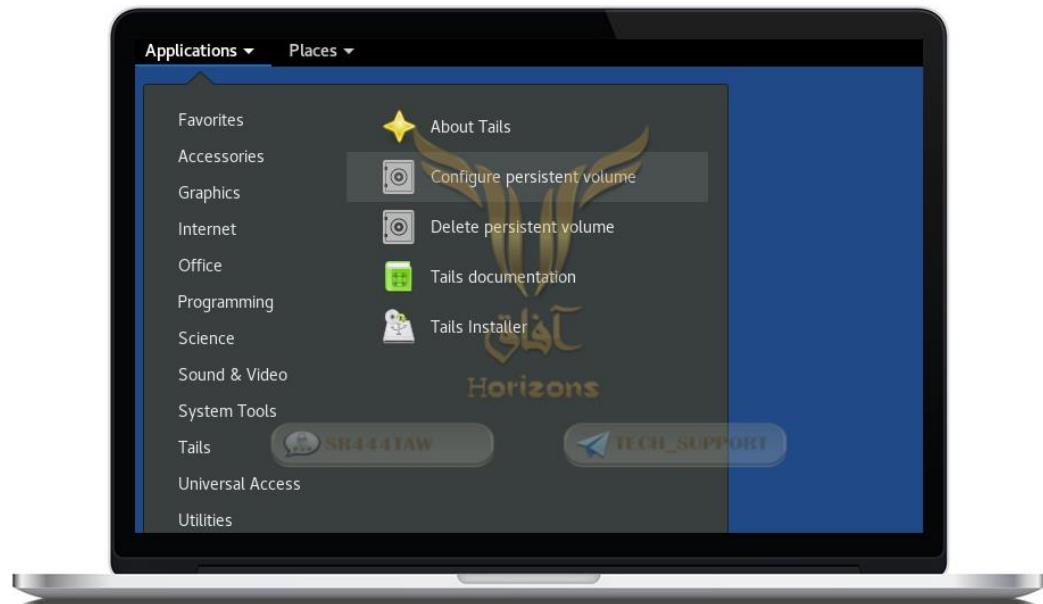




- ملاحظة: في حالة واجهتك مشكلة بالإتصال أطلب جسور أخرى.

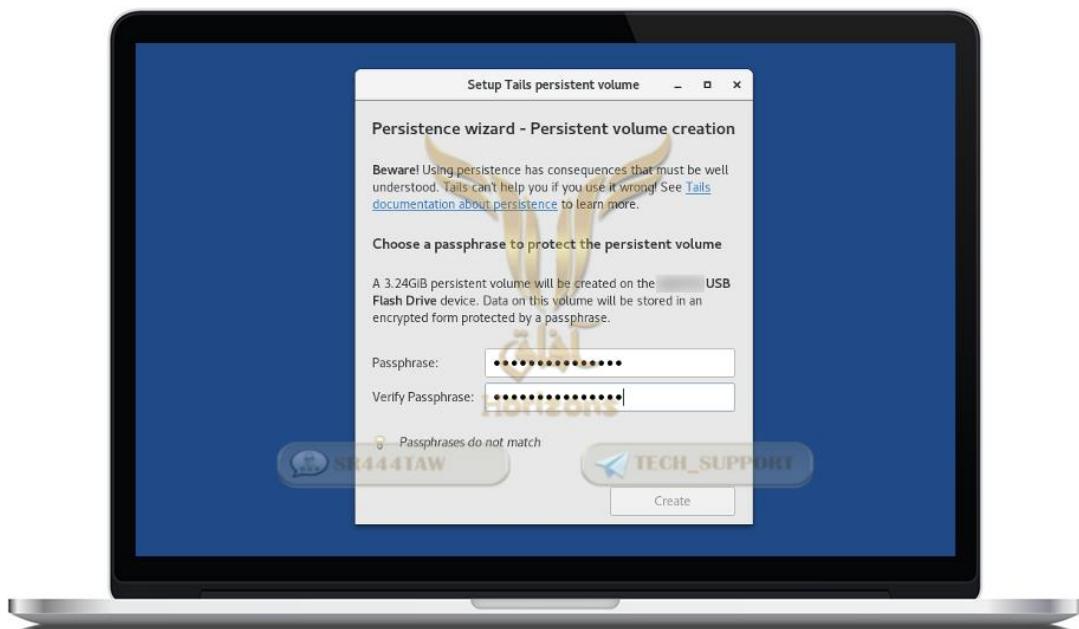
### تخصيص مساحة تخزين

Configure persistent volume من خيار Applications ثم نذهب إلى خانة Tails

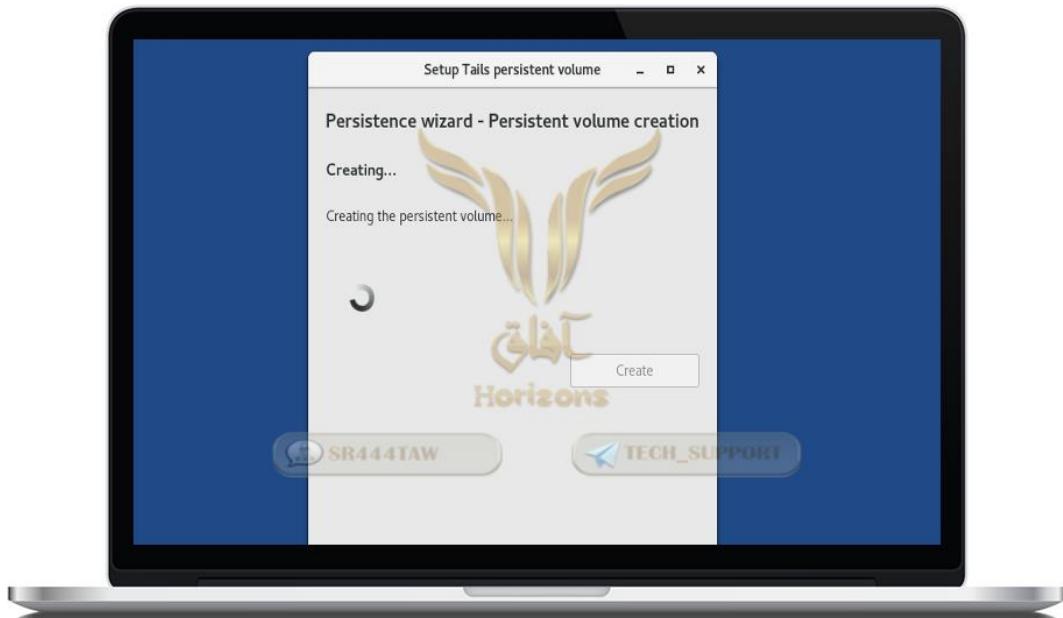


نختار كلمة سر لتشفيir مساحة التخزين و يجب أن تكون طويلة تحتوي أرقام و حروف و رموز ثم نضغط





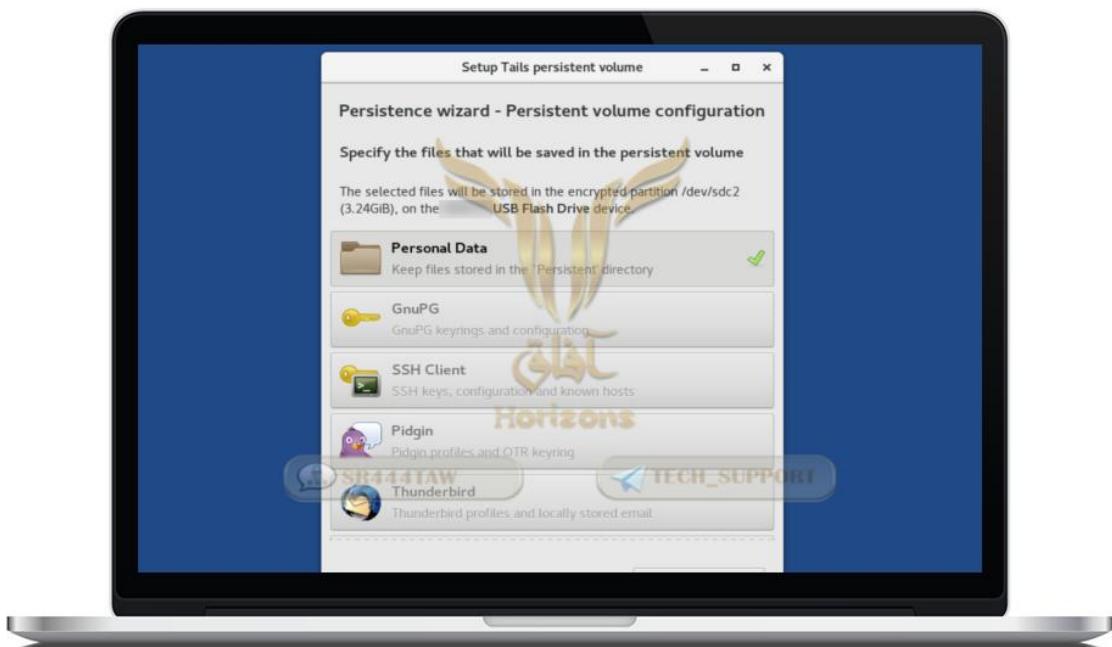
• نضغط **Create** و ننتظر



• تظهر لنا الآن قائمة فيها خيارات لتخفيض مساحة التخزين حسب حاجتك

- نختار **Personal Data** -





- ثم نضغط **Save**

وننتهي من تخصيص المساحة، عليك إعادة تشغيل تايلز  للتمكن من استعماله

## المرحلة الخامسة : نبذة عامة عن الأدوات

:Accessories خانة ◎





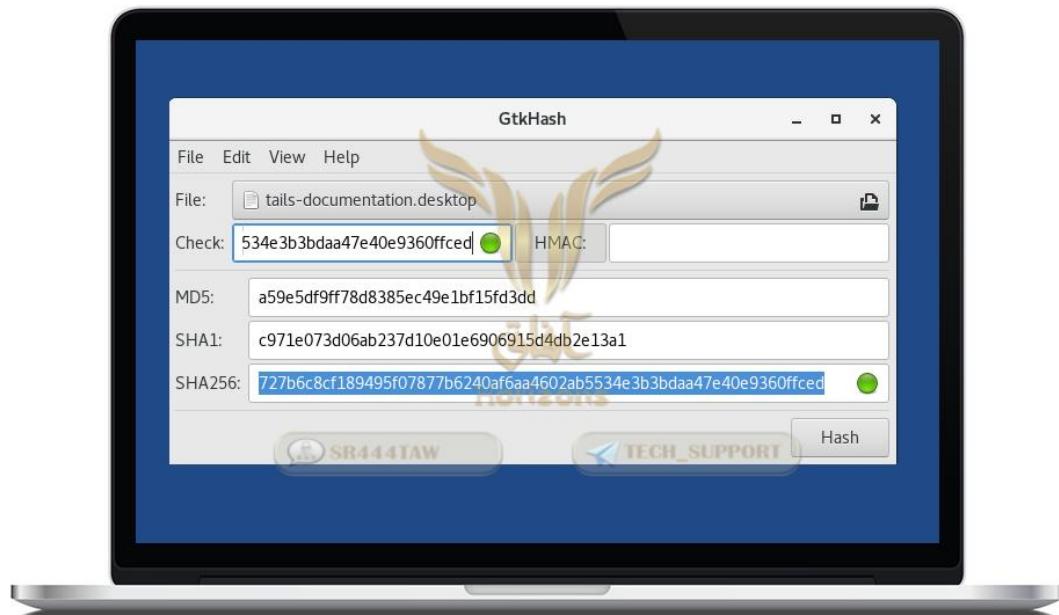
### :GtkHash -

أداة لاستخراج هاشات ملف معين بعدة صيغ: sha512، sha216، md5 (بصمة رقمية) و المقارنة بينهم

نختار الملف في خانة **File**

نضع هاش الملف الذي نأخذه من مصدره أو المرسل في خانة **Check**

ثم نضغط **Hash**



و كانت النتيجة إيجابية هنا (تطابق)



### - KeePassX -

أداة مجانية مفتوحة المصدر تمكن المستخدم من حفظ كلمات المرور بسهولة وأمان حيث تتيح لك الأداة حفظ كلمة مرور واحدة فقط ومن ثم أقوم بإنشاء قاعدة بيانات مشفرة لحفظ جميع كلمات المرور التي تستخدمها على النظام، لمعرفة المزيد حول [KeePassX](#)

(ننوه أنه يجب عليك حفظ المستودعات في مساحة تخزين كونها ستضيع إذا أعدت تشغيل تايلز)

### • خانة Graphics :



- وفيها برامج تصميم بصفة عامة:

**adobe photoshop** على لينكس **gimp**-

**adobe illustrator** بديل برنامج **inkscape**-

**adobe indesign** بديل لبرنامج **Scribus**-

### • خانة Internet :

### - TOR BROWSER -

يربط اتصالك بشبكة تور وبخفي موقعك الجغرافي حيث يمكنك استخدام شبكة الإنترنت بتخفٍ و بعيداً عن الرقابة الإلكترونية من قبل مزودي

الخدمة أو الحكومات لمعرفة المزيد حول متصفح تور [هنا](#)



يأتي مع متصفح التور عدة إضافات للحفاظ على الخصوصية منها:

**Torbutton**: أداة خاصة بمتصفح التور لمعالجة هجمات **Cookies** واستعمال **JavaScript** بأمان.

**HTTPS Everywhere**: أداة لتفعيل بروتوكول التشفير **SSL** لغالبية المواقع.

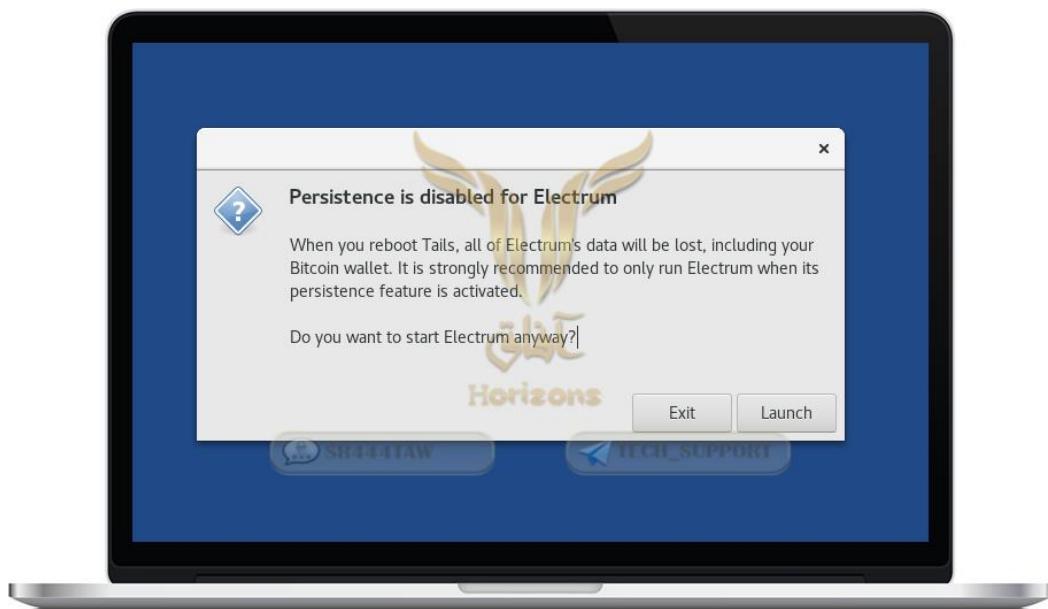
**NoScript**: أداة للحصول على تحكم أكبر في صلاحيات **JavaScript** وبإمكانك منعها والسماح لعناصر محددة.

**uBlock Origin**: أداة لمنع الإعلانات وروابط التتبع المدمجة بالموقع، تمنع كذلك هجمات التعدين.

### Electrum Bitcoin Wallet

محفظة آمنة بسيطة لإدارة عملة البيتكوين يمكن الاستقبال والإرسال بها خفيفة وتدعم التخزين البارد (**Offline**)

عند تشغيلها تظهر رسالة تحذر من أن أي عملات تستقبلها ستضيع عند إعادة التشغيل ما لم تحفظها بمساحة تخزين.

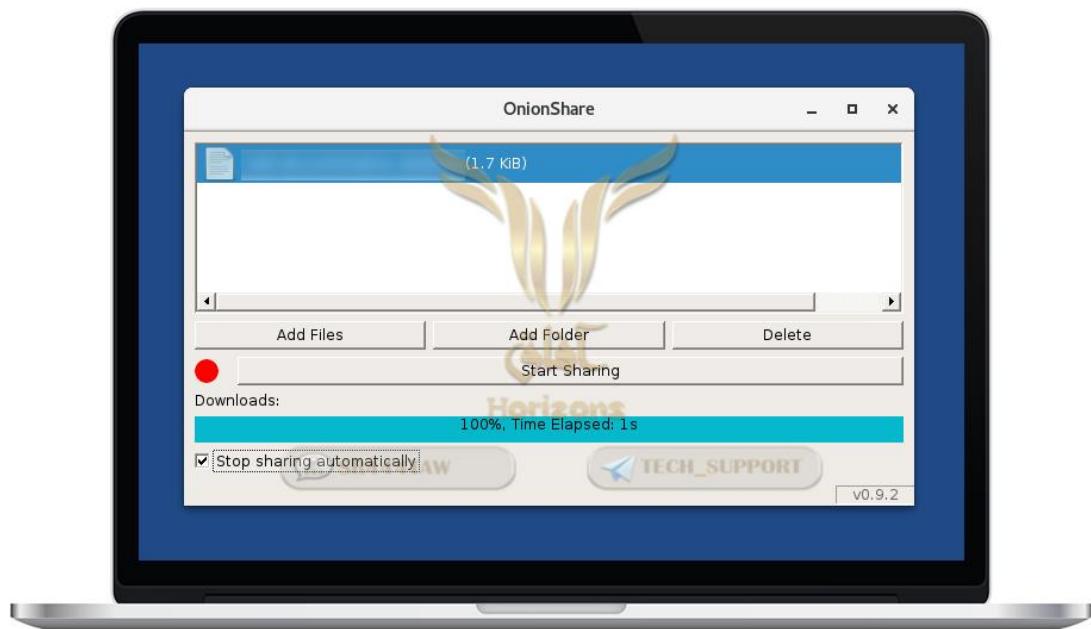


للاستزادة [اضغط هنا](#)

### OnionShare -

أداة بواجهة رسومية لمشاركة الملفات ورفعها عبر شبكة التور .

- نختار الملف المراد مشاركته عبر الضغط على **Add File**

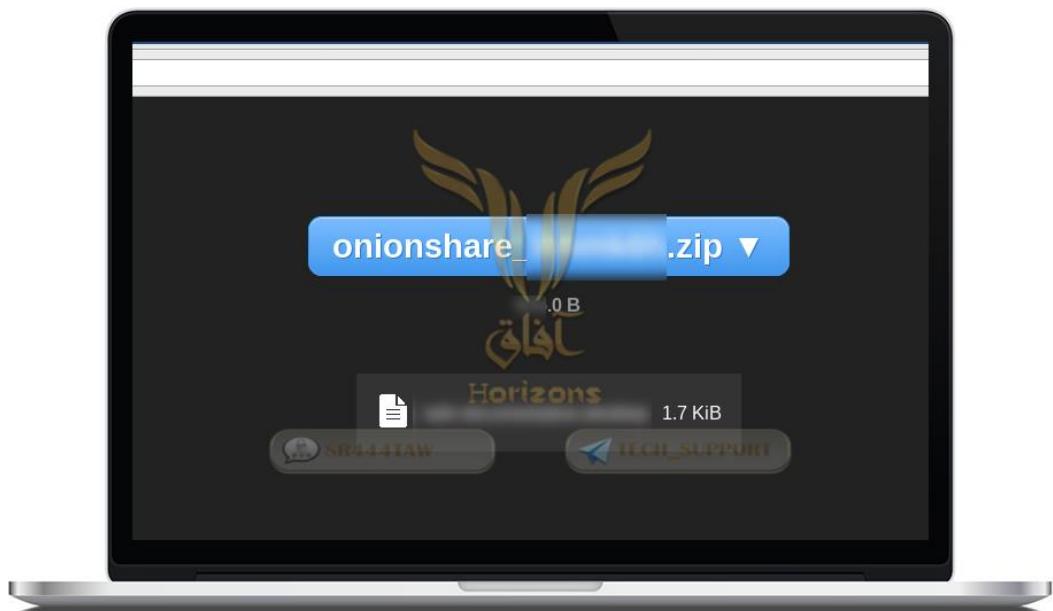


- ثم نضغط **Start Sharing**



- يظهر لنا رابط ننسخه عبر الضغط **Copy URL** و نرسله للشخص المراد أن يحمل الملف.





بإمكانك عندما يستلم الشخص ملفك و يحمله أن تلغى نشره **Stop Sharing** أو حذفه **Delete File**.

**OnionShare**: أحد أحسن الطرق لمشاركة الملفات لكن يبقى يواجه العديد من التهديدات الأمنية والمشاكل فيفضل إرسال الملفات الصغيرة والمشفرة مسبقاً.

#### **Pidgin internet messenger**

تطبيق للمحادثات المشفرة حر المصدر و يمكن إدارة عدة حسابات باستعماله، يدعم بروتوكولات التشفير OTR و Omemo.

للاستزادة تجد الشرح بالعربية [هذا](#)

و بالإنجليزية [هذا](#)

#### **: Thunderbird -**

برنامج غني عن التعريف حر مفتوح المصدر من تطوير **mozilla** لإدارة الإيميلات من سطح المكتب يأتي مع إضافة **Enigmail** لدعم

بروتوكول **OpenPGP** وننصح باستعمال الإيميلات من واجهات الويب (الموقع الرسمي).

#### **:Unsafe Browser**

متصفح غير آمن لا يرسل الترافيك عبر شبكة التور، ننصح بعدم استعماله إلا للحالات القصوى.



• خانة Systeme Tools



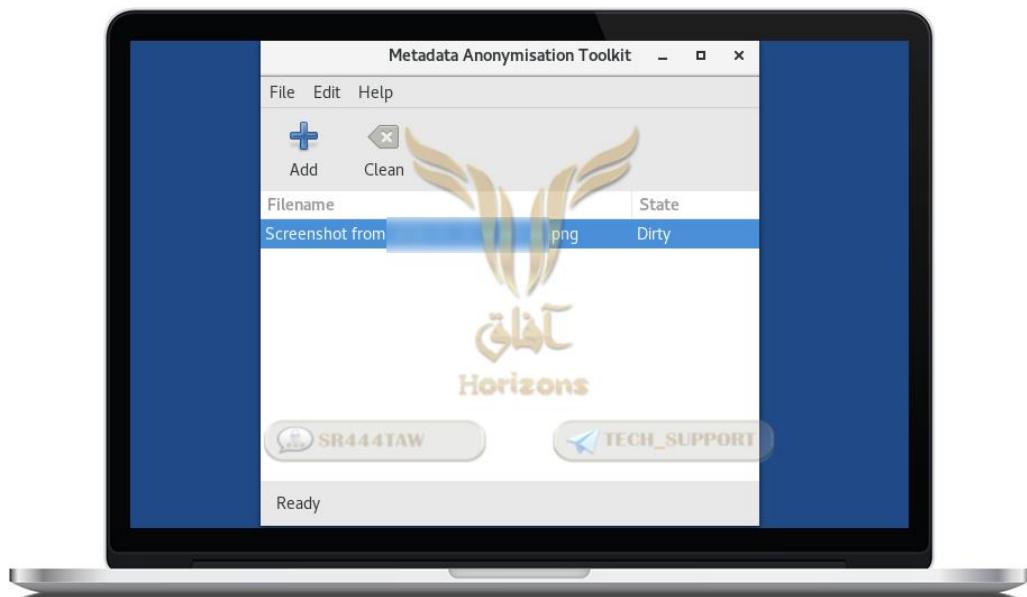
: (Metadata Anonymisation Toolkit (MAT-

-أداة لحذف البيانات الوصفية من الصور و الوسائط الأخرى كبيانات الموقع وقت الإلتقاط وغيرها).



-نقوم بفحص أحد الصور





وَجِدْنَا هَا مُلُوَّةً، 'clean' نَصْغِطُ لَحْذَفِ الْبَيَانَاتِ الْوَصْفِيَّةِ



لِلْعِرْفَةِ أَكْثَرَ عَنْ خَطَرِ الْبَيَانَاتِ الْوَصْفِيَّةِ



**سلسلة الوعي الأمني**  
البيانات الوصفية (METADATA)

**البيانات الوصفية** هي المعلومات حول الإتصالات التي ترسلها وتستقبلها ، تشمل البيانات الوصفية كل شيء في العالم الرقمي وعلى شبكة الانترنت حيث تعتبر البيانات الوصفية بمثابة غلاف للمحتوى حيث تصف الموضوع العام للبريد الإلكتروني ومدة محادثتك و من المستقبل ومن المرسل والمكان الذي تتصل منه وهوية الشخص الذي تتصل به ، البيانات الوصفية غالباً ما تصف كل شيء ماعدا محتوى إتصالاتك كمحتوى البريد الإلكتروني او محتوى المكالمة الهاتفية .

**معظم الحكومات العربية والغربية** تستخدم البيانات الوصفية في ايجاد خيوط لتعقب الجهاديين حيث تحصل هذه الحكومات على سجل الاشخاص الذين اتصلت بهم الشهر الماضي ومتى اتصلت بهم وain موقعك الجغرافي حينها وموقع مستلم المكالمة ، حصول الحكومات على البيانات الوصفية يعترف اسهل لهم من حصولهم على المحتوى نفسه

يمكن مجرد عينة صغيرة من البيانات الوصفية ان تتحول الى **عدسة كاشف** لحياة شخص ما بل في بعض الاحيان تكون البيانات الوصفية سببا في اعتقال الاخوة والاخوات او قصدهم

إن حماية البيانات الوصفية من الجمع من قبل جهات خارجية مشكلة صعبة تقنياً لأن أطراف ثلاثة غالباً ما تحتاج للوصول للبيانات الوصفية لتوصيل اتصالاتك بنجام. **مثلاً** يحتاج ساعي البريد لقراءة العنوان على طرف البريد، يتوجب تعلم **اتصالات الرقمنة** بالمرسل والوجهة. تحتاج شركات الاتصالات الى معرفة الموقع التقريري لهاتفك لتوجيه المكالمات اليه

استخدم خدمات مثل شبكة تور **Tor** ومشاريع تجريبية مثل **Ricochet** للحد من البيانات الوصفية الناجمة عن طرق التواصل التقليدية على الانترنت. أفضل ما يمكن فعله هو معرفة البيانات الوصفية المرسلة عند التواصل مع الآخرين والجهات التي تستطيع الوصول إليها وكيف يمكن استخدامها.

### tails installer -

أداة خاصة بتوزيعة تايلز تقوم بنسخ التوزيعة التي تستعملها لمفاتيح **USB** أخرى.

**:TERMINAL**



الطرفية عبارة عن واجهة يتيح لك التعامل مع النظام من خلال سطح الأوامر وتكون أدوات الإدخال "لوحة مفاتيح" فقط .

هذا ممكّن بـ "Terminal Emulator": وهو برنامج يكون في الواجهات الرسومية وظيفته تنفيذ الأوامر في الشل "Shell".

إذن الطرفية هي وسيلة تواصل مع الشل ويمكن لمحاكي الطرفية الرسومي أن يستخدم الفأرة لتنفيذ مهام نصية فقط كالنسخ واللصق، تستطيع من خلال الطرفية التحكم بالنظام كاملاً وتتمكن هنا قوة الطرفية فمن خلالها يمكنك على سبيل المثال "ثبتت ببرامج - تعريف العتاد - إدارة المستخدمين - إدارة الملفات ... لمعرفة طريقة ثبيت البرامج من خلال الطرفية اضغط [هنا](#) أو [هنا](#) أو [هنا](#) أو [هنا](#) لا ننسى الغير متمنك في أوامر البash Bash من استعمالها.

PGP لمفاتيح الرسمية الواجهة

**كلمات السر ومفاتيح التعمية (Seahorse):** هي الواجهة الرسمية لبروتوكول التشفير PGP بروتوكول PGP اختصار لـ Privacy Good Pretty ( Philip Zimmermann ) طوره فيليب زيمerman عام ١٩٩١ وهو حاصل على البكالوريوس في علوم الحاسوب من جامعة أطلنтика في فلوريدا حصل زيممان على جوائز عديدة في مجال تكنولوجيا المعلومات وحقوق الإنسان، لعمله الرائد في تشفير وأمن المعلومات وصنفته العديد من المجلات ضمن فئة الأشخاص الذين كان لهم أبرز الأثر في تطوير استخدام شبكة الإنترنت.

يعتمد تشفير البريد الإلكتروني باستخدام بروتوكول PGP على أزواج المفاتيح Key Pairs كل زوج من المفاتيح يتكون من مفتاح سري Key Secret ومفتاح عام Key Public: وهو عبارة عن ملفان يمكن الاحتفاظ بهما على القرص الصلب أو على USB يرتبط زوج المفاتيح بعنوان بريد الإلكتروني ويستخدمان لتشفيه وفك تشفير الرسائل المرسلة من ذلك العنوان وإليه لذلك ستحتاج الملفين أينما أردت تشفير وفك تشفير الرسائل.

وضع المفاتيح (الملفين) على USB ميموري يسهل موضوع نقل الملفات إلى الأجهزة كي يستطيع الآخرون فاك تشفير الرسائل المشفرة التي ترسلها إليهم يجب أيضاً أن ترسل لهم مفتاحك العام وأيضاً أن تمتلك مفاتيحك العامة من هنا تأتي تسمية المفتاح العام فهو المفتاح الذي تعطيه لشخص آخر ليفك تشفير رسالة تم تشفيرها خصيصاً له بالاعتماد على زوج مفاتيحك وعلى مفتاحك العام بينما يبقى مفتاحك السري ملكاً لك وحدك، لا تشاركه مع أي شخص كان وتحمييه من الوقوع بيد أي شخص آخر.

كما قلناً سابقاً، لإرسال رسالة مشفرة إلى شخص ما يجب أن يتتوفر لدى المرسل مفتاحه العام. من الممكن أن يرسل ذلك الشخص مفتاحه العام إلى المرسل بدون تشفير عبر البريد الإلكتروني، أو يمكن أن ينسخ ملف مفتاحه العام على USB ورسله.

المهمهو التأكيد أن ذاك المفتاح العام مرتبط مع عنوان البريد الإلكتروني ذاك وأنهما فعلاً ملك الشخص الذي تنوی من إسلته

بروتوكول **PGP** لا يعتمد على تشفير الرسائل فقط بل يمكنك استخدامه في تشفير الملفات والمستندات أيضاً وتوجد العديد من الواجهات الرسمية لبروتوكول **PGP** أبرزها واجهة أو أداة **Seahorse** الموجودة بنظام تايلز والتي ستباع شرحها الآن ياذن الله

- اضغط على الأيقونة التالية + لإنشاء مفتاح PGP



- اختر **PGP Key** من القائمة التالية -



.اضغط على **Advanced key options**

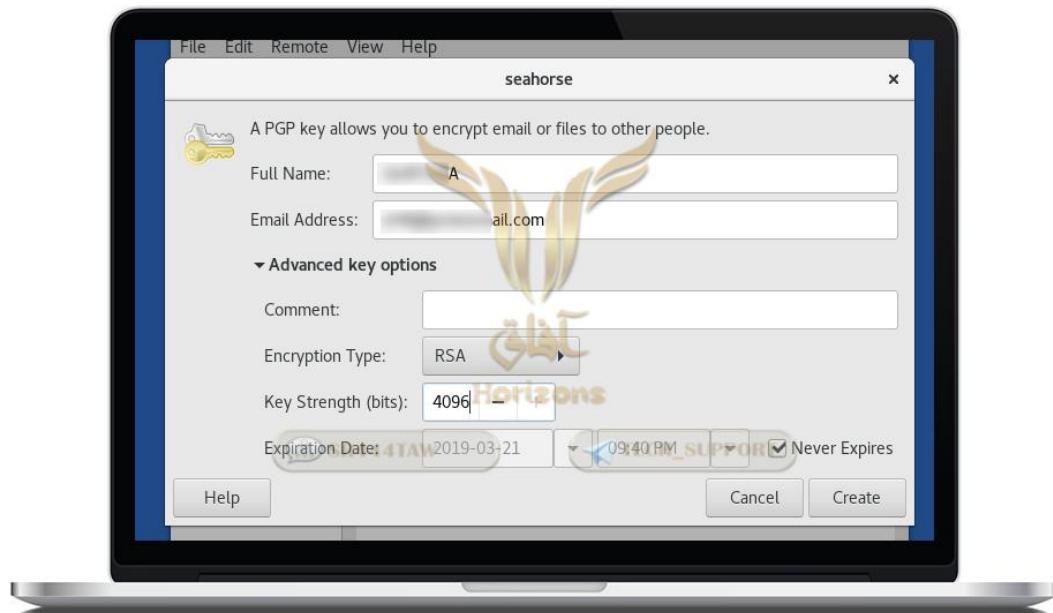
اكتب اسمك الرمزي - و ليس الحقيقي - **(Full Name)**

**البريد الإلكتروني** **(Email Address)**

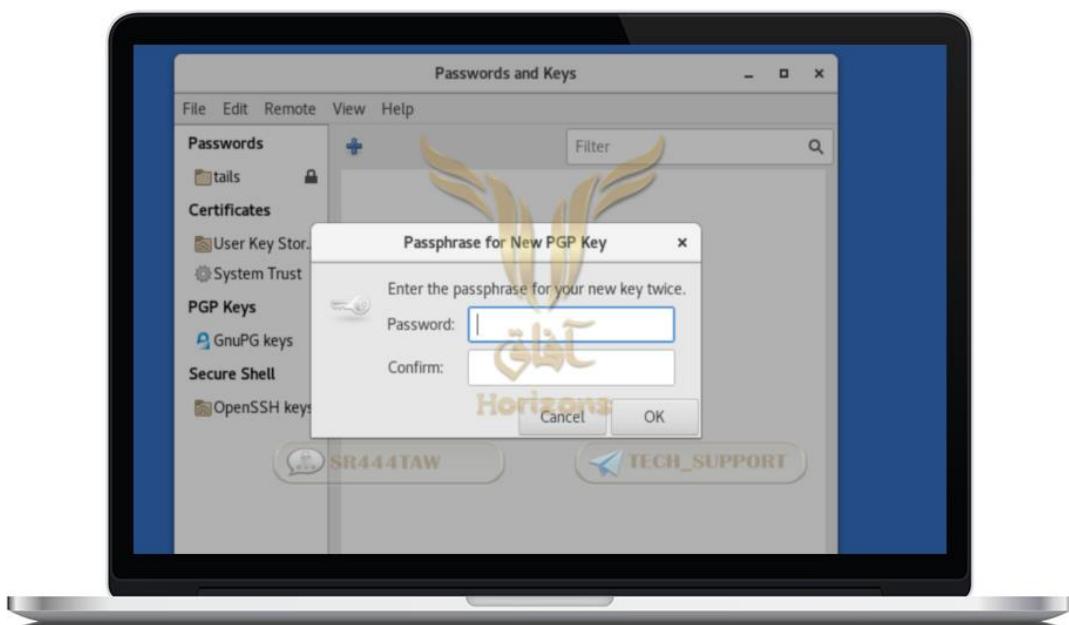
اجعل طول المفتاح **٤٠٩٦**

و يمكنك إضافة وقت معين لنتهاء صلاحية المفتاح عن طريق **(Expiration Date)**





-عین کلمة سر قویة تتكون من ۲۰ عنصر تحتوي علی حروف كبيرة وصغيرة وأرقام ورموز واضغط YES واحفظها في مكان آمن.



- انتظر قليلاً و سيظهر المفتاح الخاص بك في قائمة GNUPG بإذن الله.





- هناك طريقتين للتواصل مع أصدقائك أو إخوانك إما عن طريق البحث عن البريد الإلكتروني أو اسم المفتاح في سيرفرات **OpenPGP**.

#### ◊ الطريقة الأولى : تصدير واستيراد ملف المفتاح العام ◊

- من قائمة **GNUPG** بإمكانك حفظ المفتاح العام الذي أنشنته عن طريق الضغط عليه ثم **<File> Export** و بإمكانك إرساله لمن تريد التواصل معهم أما بالنت أو مفاتيح **USB**.



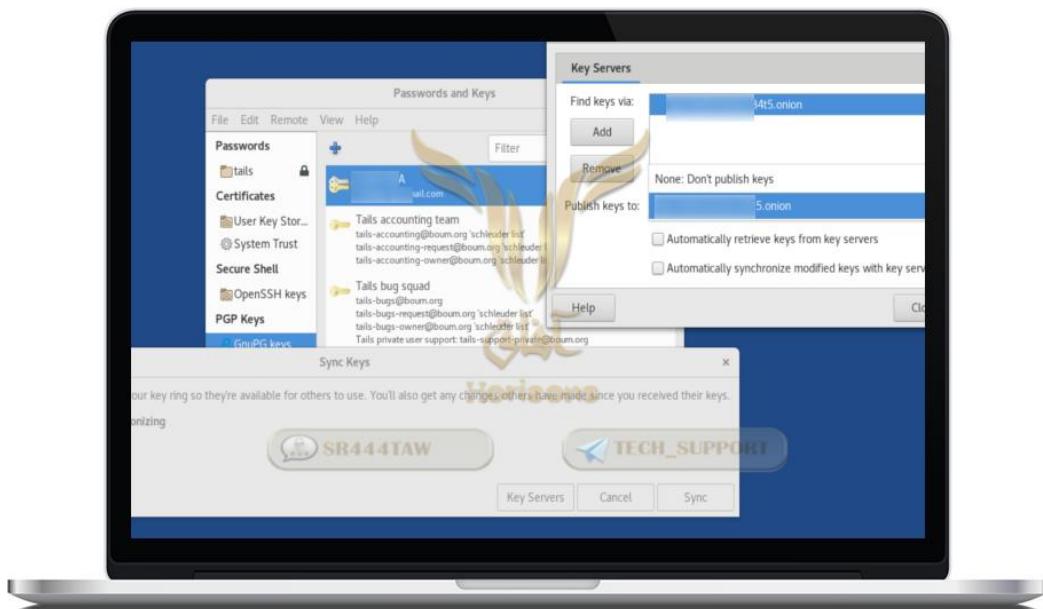
- ثم نحفظ المفتاح في المسار الذي نريد.  
- أما لإستيراد مفتاح عام فاضغط على **<File> import**

#### ◊ الطريقة الثانية: مزامنة المفتاح العام مع سيرفرات PGP ◊

• أولاً يجب أن يكون الطرف الثاني قد زامن مفناحه مع السيرفرات حتى تستطيع البحث عنه

إذا أردت مزامنة مفناحك مع سيرفرات OpenPGP اضغط على **Sync and publish keys** ثم **Remote**

- اضغط على **Key servers**



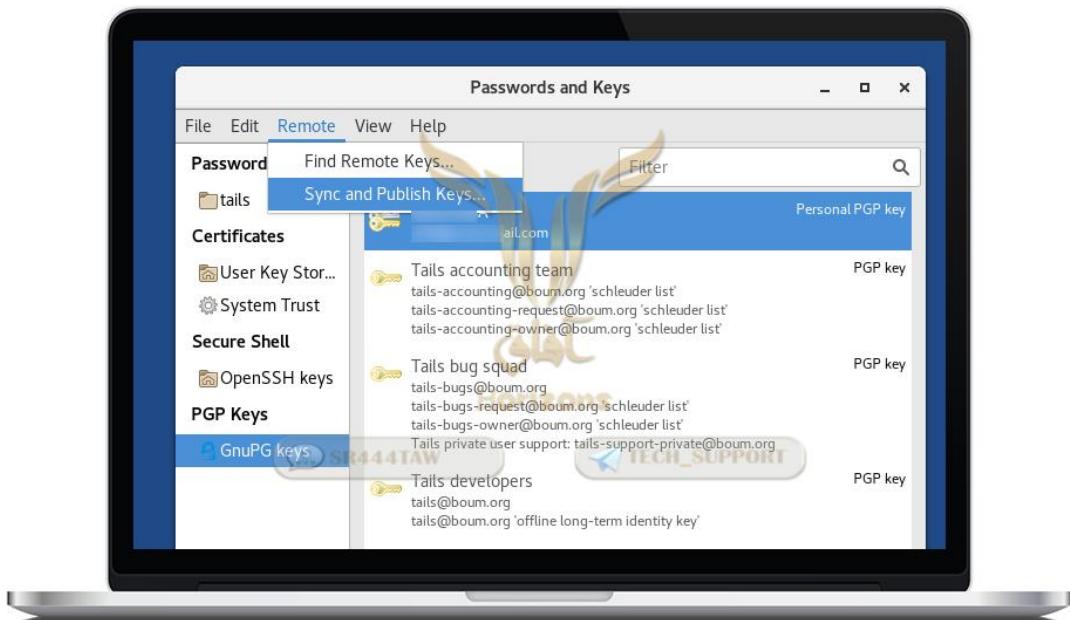
• يمكنك اختيار السيرفر أو الخادم الذي تريده مزامنة مفناحك العام عليه مثل **hkp://pool.sks-keyservers.net** أو **hkps://pgp.mit.edu**

**ملاحظة:** يجب على الطرف الثاني الذي يبحث عنك أن يرفع مفناحه على نفس السيرفر حتى تتمكن من إيجاده.

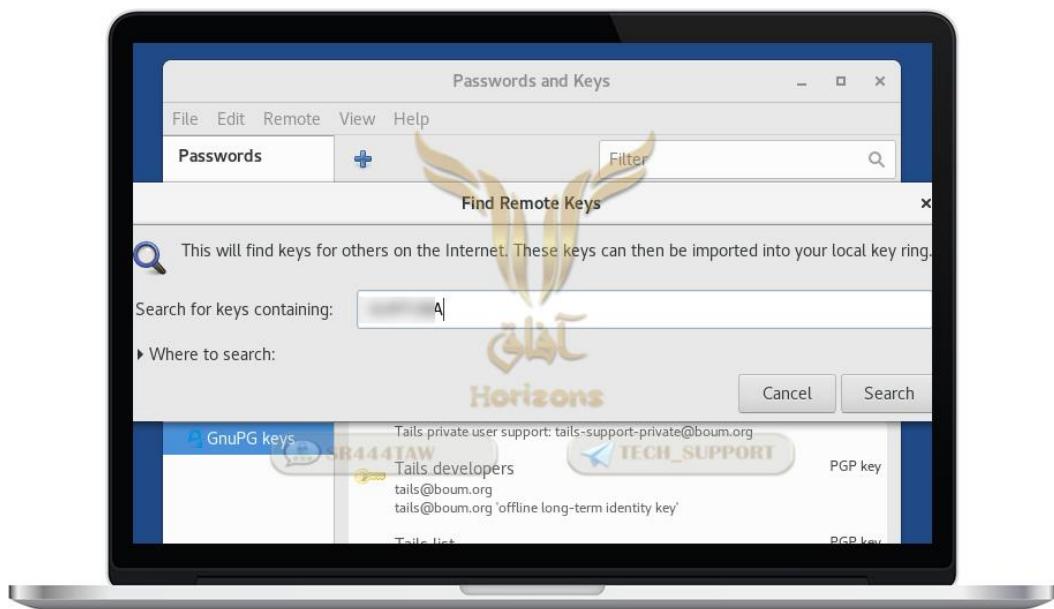
- ثم اضغط **Sync** لبدء مزامنة مفناحك العام.

بعد أن زامنت مفناحك العام بإمكانك أيضا تحميل مفاتيح المراد الإتصال بها بشرط أن يكونوا في نفس السيرفر الذي رفعت عليه مفناحك.

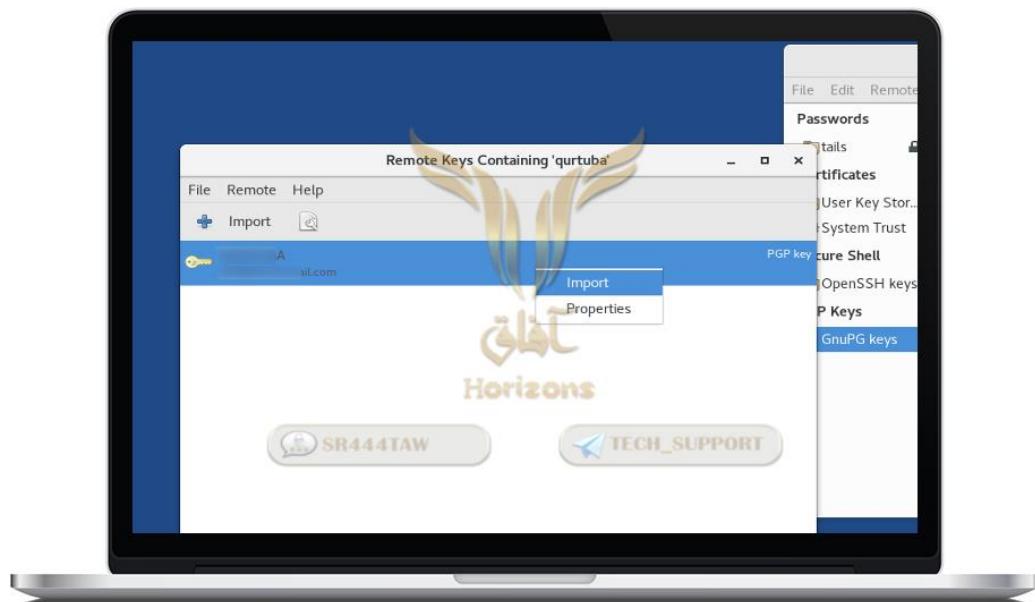
- اضغط على **Find remote keys** ثم **Remote**



-ثم اكتب البريد الإلكتروني أو اسم المفتاح للطرف الثاني المراد التواصل معه واضغط " Search "



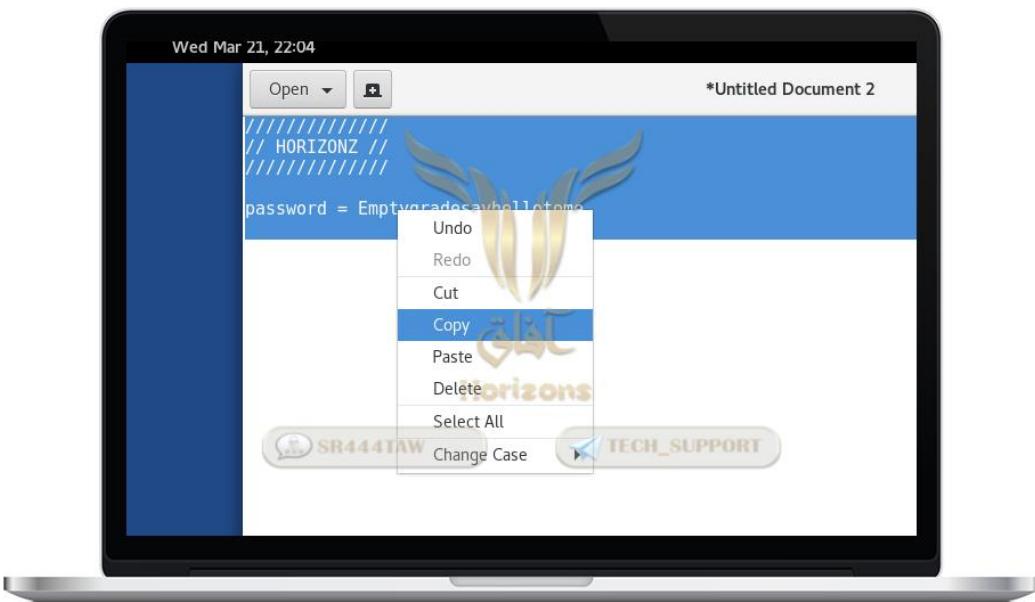
- ستظهر لك المفاتيح المتعلقة بالبحث تحقق من البريد الإلكتروني واسم المفتاح جيداً ثم حدهه واضغط " IMPORT "



### تشفير و فك تشفير الملفات و الرسائل المشفرة ببروتوكول

#### - PGP - تشفير الرسائل ببروتوكول

- الآن اضغط بالزر الأيمن للماوس على أيقونة الحافظة بشرط المهام واختر " Open TEXT EDITOR " نكتب النص المراد إرساله و ننسخ

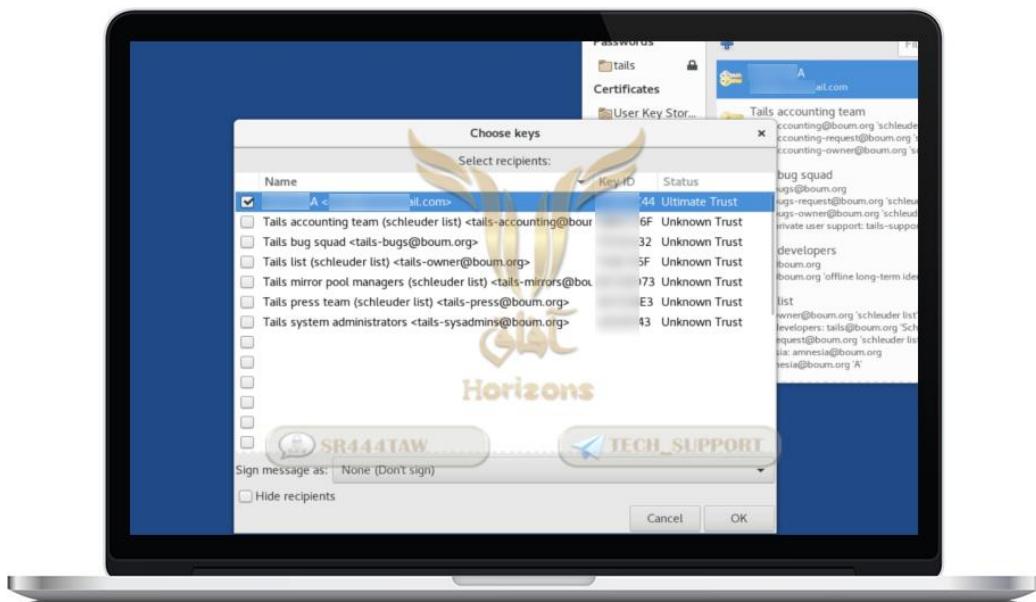


- اضغط على أيقونة الحافظة بشرط المهام واختر "Sign/Encrypt Clipboard with Public Keys"



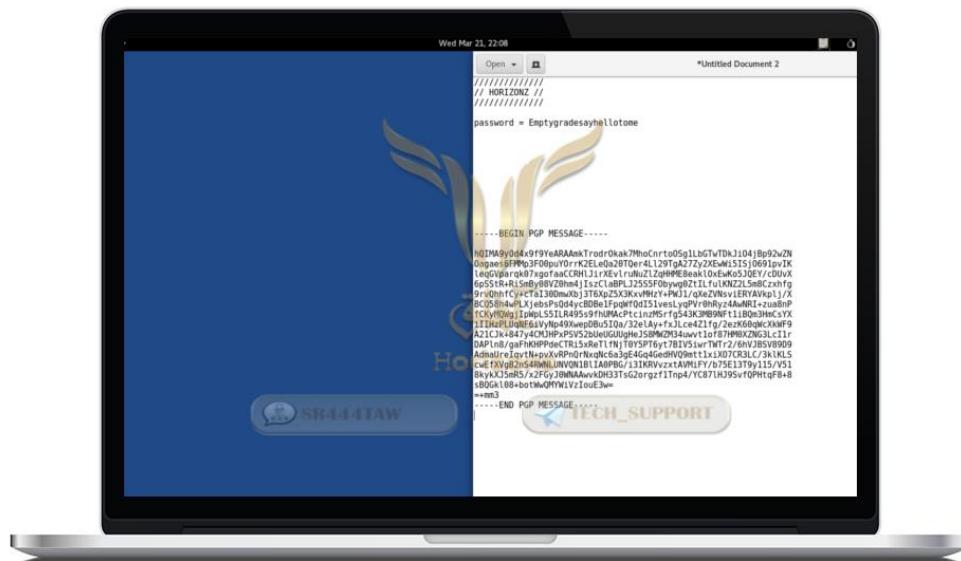


- اختر المفتاح العام للطرف الثاني (المراد إرسال الرسالة له) ثم اضغط "OK"



- عد الآن إلى **Text Editor** واعمل لصق لتجد الرسالة مشفرة.

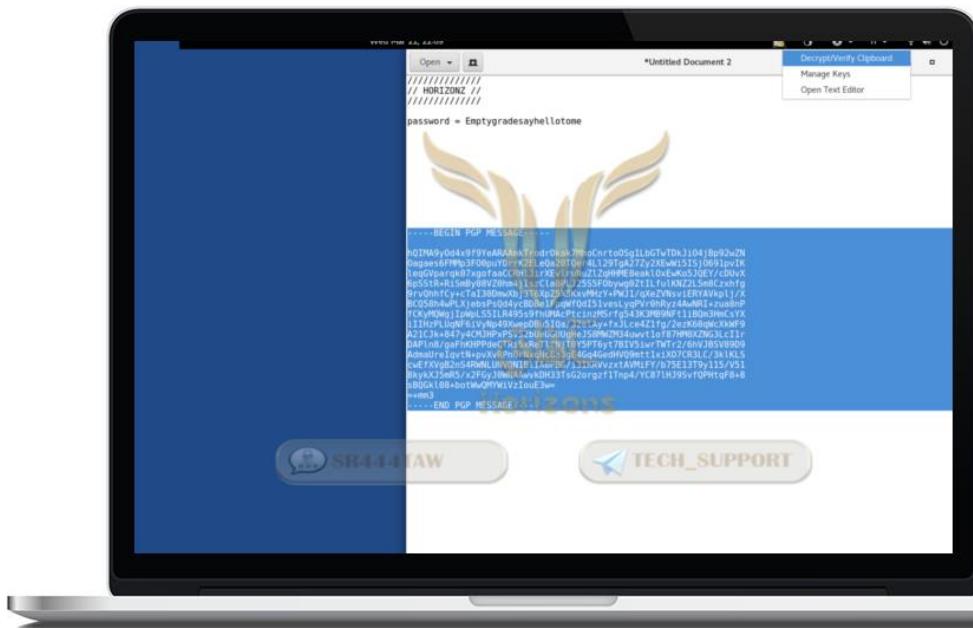




- و هاهي الرسالة المشفرة ببروتوكول **PGP** أسفل الرسالة الأصلية (الغير مشفرة) كل ماعليك فعله الان هو إرسال هذه الرسالة للطرف الثاني من خلال تطبيقات التواصل الاجتماعي أو البريد الإلكتروني.

#### - فك تشفير رسالة ببروتوكول PGP

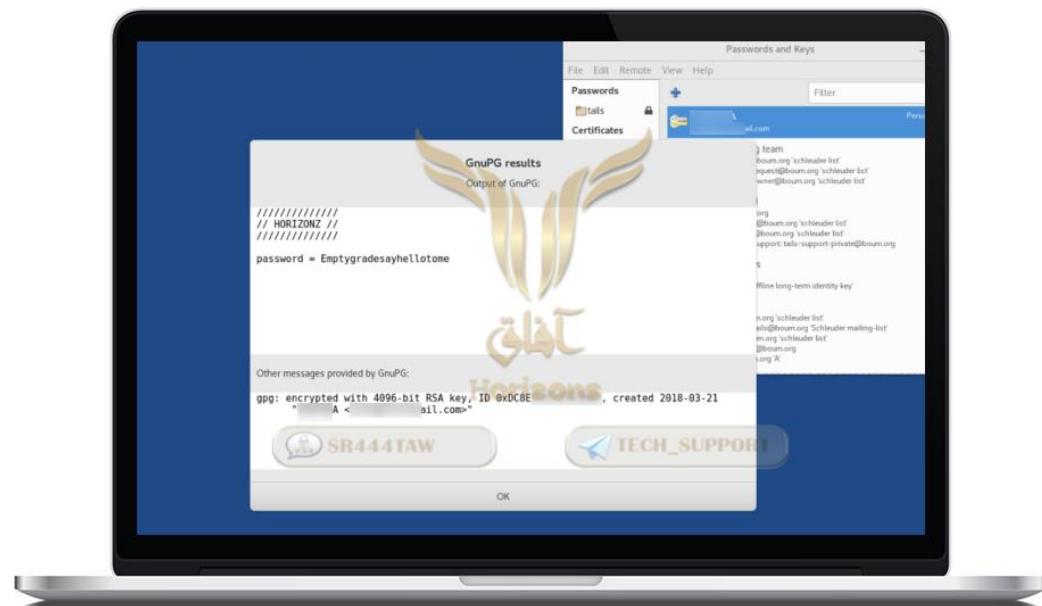
- ◎ الطرف الثاني سيرسل لك رسالة موقعة بـ **مفتاحك العام** كالرسالة في الصورة السابقة لذا قم بنسخ الرسالة بالكامل واضغط على أيقونة الحافظة بشرط المهام واختر "Decrypt/Verify Clipboard"



- ◎ سيسطّلب منك النظام كلمة المرور لمفتاح **PGP** الخاص بك التي عينتها أثناء إنشاء المفتاح.

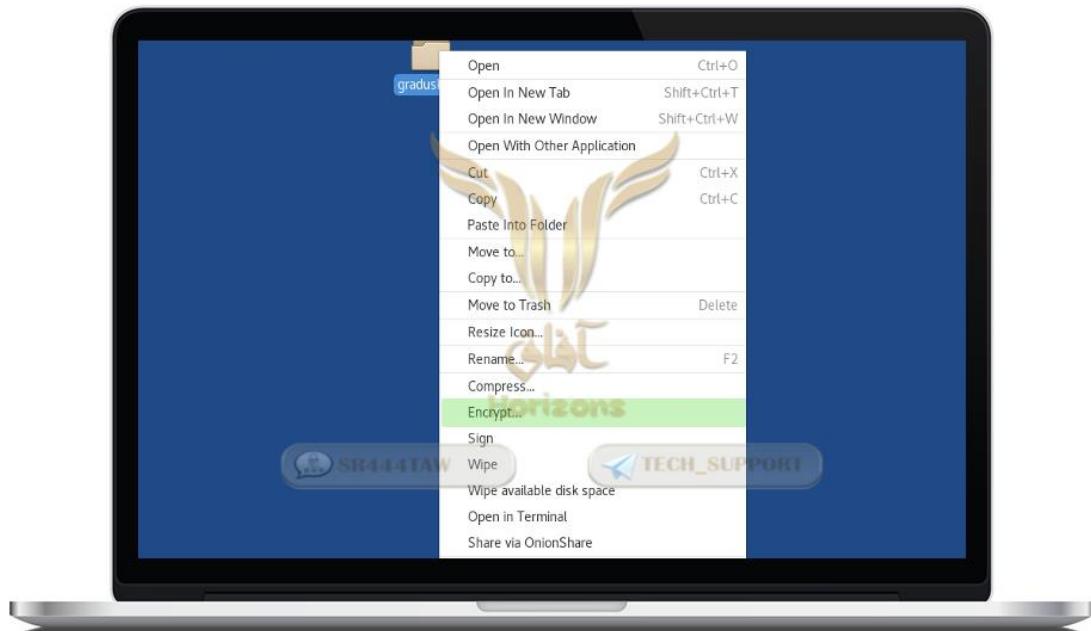
- ثم تظهر لك الرسالة بعد فك تشفيرها بهذا الشكل.





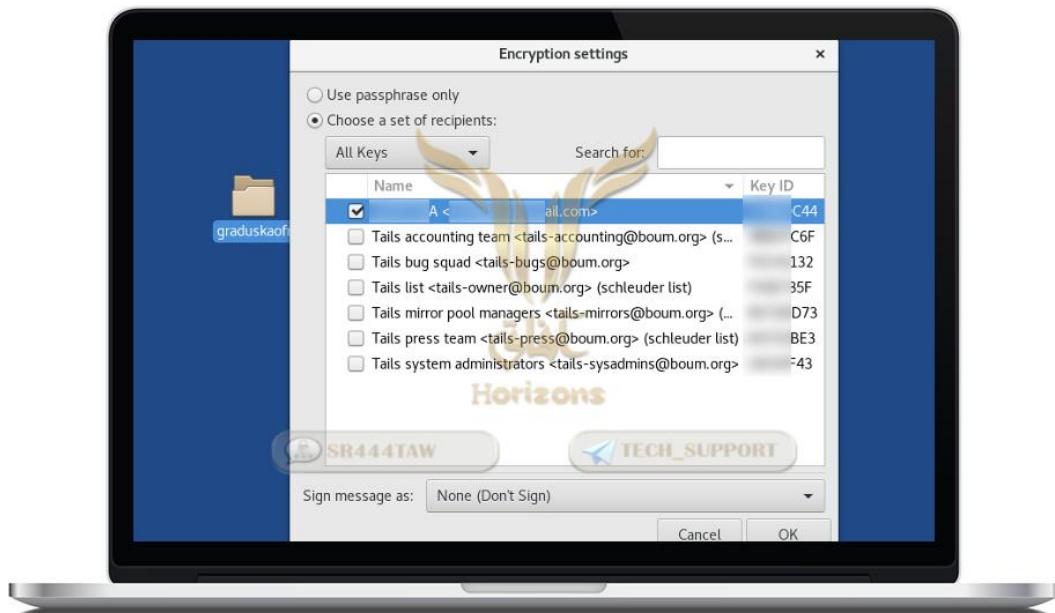
## - شرح تشفير ملف بـاستعمال بروتوكول PGP -

- ◎ اذهب إلى الملف المراد تشفيره واضغط بزر الماوس الأيمن واختر "Encrypt"



- ◎ يمكنك كذلك تشفير الملف بواسطة كلمة سر ببساطة، هنا نشفيره بـاستعمال بروتوكول PGP:

نختار أولاً المفتاح العام "PUBLIC KEY" للطرف المراد إرسال الملف المشفر إليه  
كما قلنا سابقاً أما أن يرسل لنا المفتاح أو نبحث عليه في السرفر الذي رفعه إليه)



- إذا كنت تري تشفير مجلد فسيطلب منك الاختيار بين تشفير كل مجلد على حدة (خيار أول) أو جمعهم في ملف مضغوط (خيار ثانى) مع اختيار اسم المجلد في "Package Name"



- الآن سيظهر لك الملف المشفر بصيغة **gpg**





- فك تشفير ملف مشفر ببروتوكول PGP

◎ نضغط يمين على الملف المشفر و نختار Open with decrypt file

(الملف يكون بصيغة .pgp)

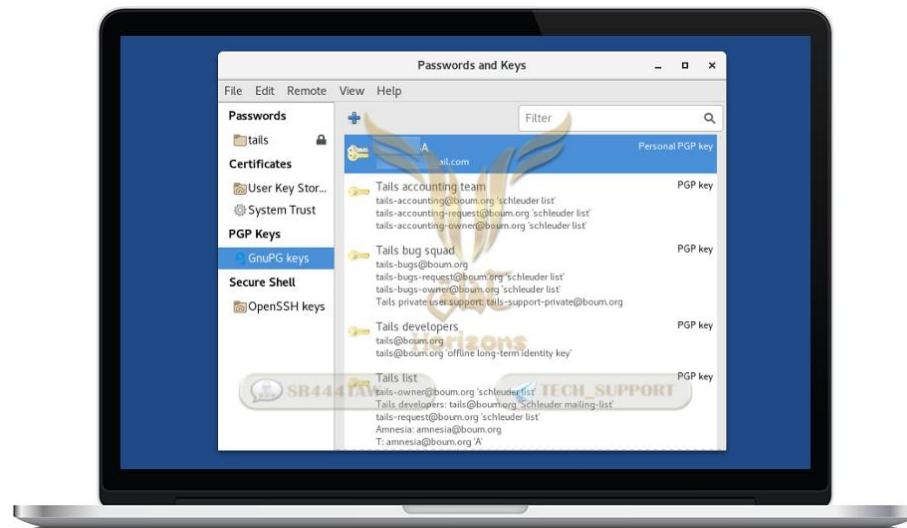


- و ستجد الملف بعد فك تشفيره بنفس المجلد بدون ppg

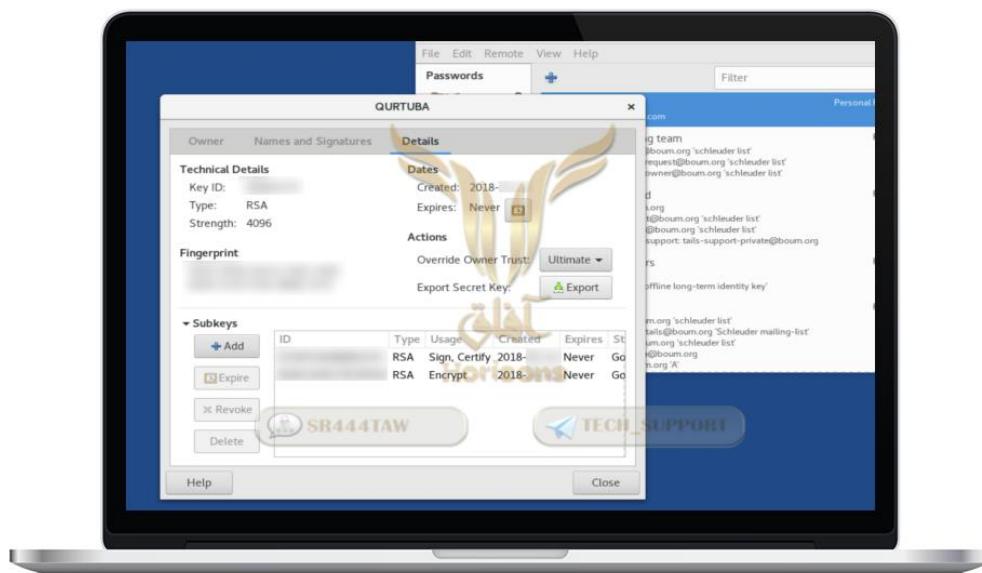
- حفظ المفتاح السري -PGP Secret Key-

- كما نعلم جميعاً أن نظام تايلز يستخدم ذاكرة الوصول العشوائي RAM فإذا أغلقت الجهاز سيتم حوّل جميع آثارك من النظام بشكل تلقائي لذا عليك بأخذ نسخة احتياطية للمفتاح السري الخاص بك ووضعه على USB أو ذاكرة خارجية أخرى غير التي استخدمتها لحرق النظام:

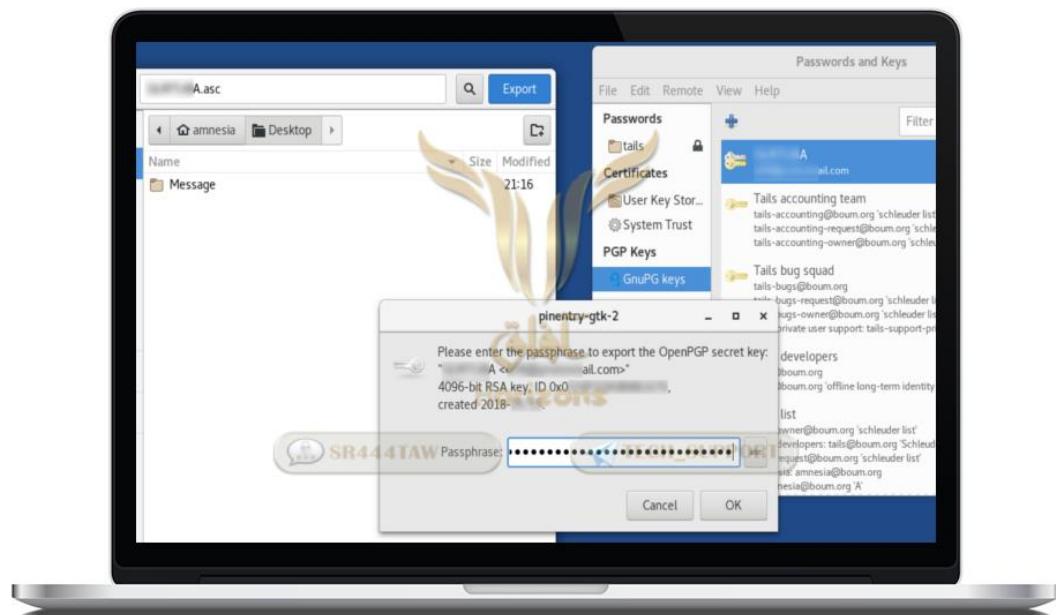
- توجه إلى **GNUPG Key** ثم اضغط على المفتاح الخاص بك ضغطتين لظهور إعداداته



- نذهب إلى **Export** ثم نضغط **Details**



- نضع كلمة السر التي وضعناها سابقاً عند إنشاء مفتاح PGP ونختار مكان حفظ المفتاح السري.

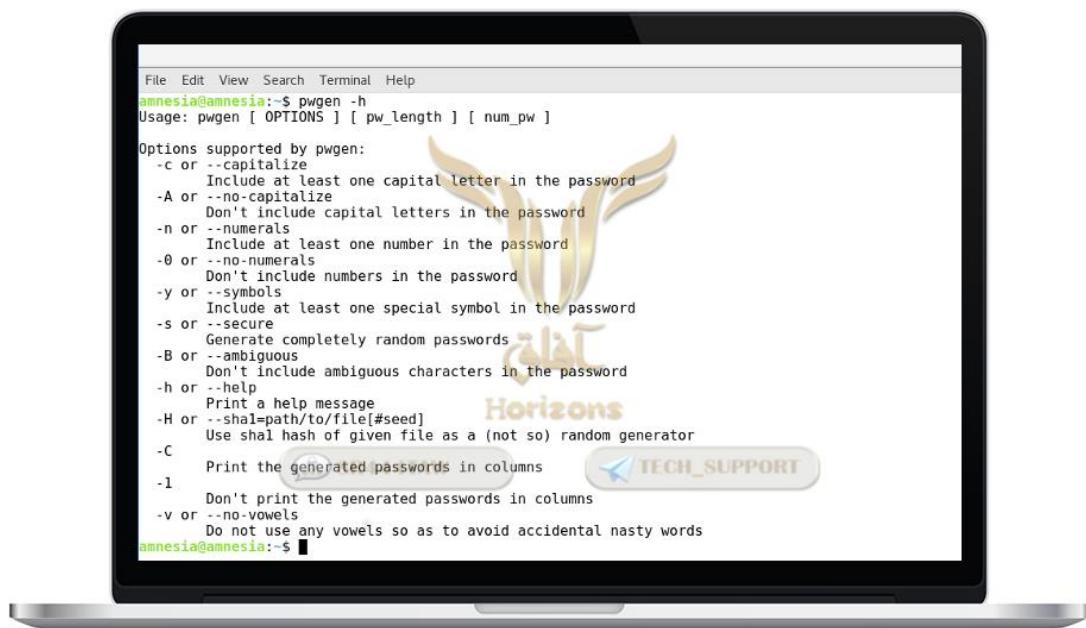


• أما لاسترجاع المفتاح السري من الذاكرة الخارجية عند استعمال النظام مرة أخرى اضغط على **import** واختر الملف وسيظهر لك ضمن قائمة مفاتيح **GNUPG**

#### • أدوات أخرى:

**PWGEN**-  
عشوانية: اختصار (Password Generator) أداة تقوم بإنشاء كلمات سر عن طريق خوارزميات

نفتح **TERMINAL** و نستدعي الأداة قائمة المساعدة بالأمر -h



نشر خواص الأداة :

[عدد كلمات السر التي تريد عرضها] [طول كلمة السر بالأحرف] [الخواص التي تريد استعمالها] **pwgen**

-c : لاستعمال حرف واحد كبير على الأقل

-A : لاستعمال الأحرف الصغيرة فقط

-n : لاستعمال رقم واحد على الأقل

-- : حتى لا يستعمل أرقام

-y : لاستعمال رمز واحد على الأقل

-s : إنتاج كلمات سر عشوائية تماماً

-h : عرض قائمة المساعدة

-C : لإظهار النتائج على شكل جدول

-1 : حتى لا يظهر النتائج على شكل جدول

-v : حتى لا يستعمل أي حرف صامتة

مثال:

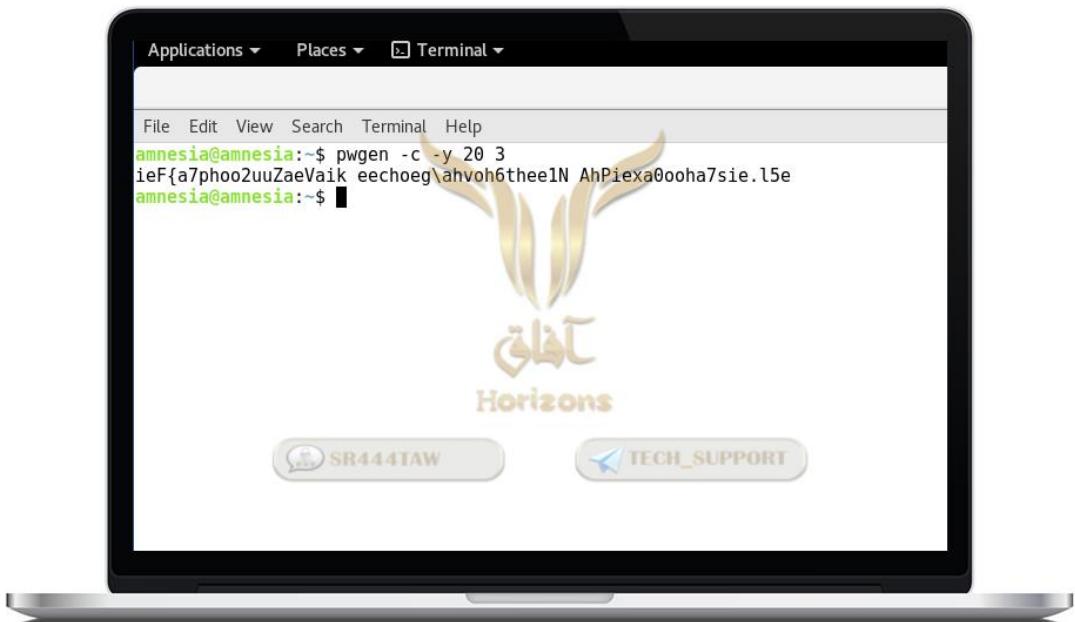
- لنسخة ٤ كلمات سر كل واحدة : تحتوي على حرف واحد كبير على الأقل + بدون أرقام + وتحتوي على رمز واحد على الأقل+تحتوي على ٢٠ حرفا

**pwgen -c -0 -y 20 4** نضع الأمر <

- لنسخة ٣ كلمات سر كل واحدة: تحتوي على حرف واحد على الأقل + تحتوي على رمز واحد على الأقل + تحتوي على ٢٠ حرفا

**pwgen -c -y 20 3** نضع الأمر <





وآخر دعوانا أن الحمد لله رب العالمين .. لا تنسونا من صالح دعائكم

\*\*\*\*\*





للتواصل:



جميع حقوق النشر محفوظة لدى مؤسسة آفاق الإلكترونية © 2018  
ولأجل نسخ المواد العلمية والأمنية التي تقدمها المؤسسة دون ذكر لمصدر

