كبسولة التخزين الآمن للملفات

كبسـولة التخزيـن الآمــن للملفـــات

مقدمة

ملفاتنا تشبه أغراضنا المادية في العديد من الأشياء وقد تكون أهمية بعض الملفات كبيرة جدا مما يستلزم منا الاحتفاظ بها بطريقة آمنة تشبه قيامنا بالاحتفاظ بأغراضنا الثمينة في خزنة سرية بمعايير أمان عالية. وفي هذه الكبسولة نهدف إلى التعريف بعدد من الأدوات التي يمكن أن تساعدنا في تخزين ملفاتنا بأمان على أجهزة الكمبيوتر أو الهواتف المحمولة.

جدول المحتويات

أولا: أجهزة الكمبيوتر

تحتوي معظم أنظمة تشغيل الحاسب طرقا لتشفير الأقراص، فإذا كان الهدف فرض تشفير كامل على بعض الأقراص أو جميع محتويات وحدة التخزين فالحل الأمثل هو استخدام الأداة المدمجة بنظام التشغيل، ولكل نظام تشغيل أداة تشفير رسمية

لأنظمة وينـــدوز يمكن استخدام **BitLocker**

لأنظمة macOS يمكن استخدام **FileVault**

لأنظمة لينكـــس يمكن استخدام **LUKS**

VeraCrypt

ويمكن كذلك استخدام برنامج VeraCrypt لتشفير الأقراص ووحدات التخزين، وهو يعمل على أنظمة ويندوز وmacOS ولينكس وغيرها، ويمكن لبرنامج فيراكريبت إنشاء مجلدات مشفرة ينشئها المستخدم ويختار كيف تبدو للمستخدمين الآخرين قبل فتحها، وبعد فتح ذلك المجلد يظهر على شكل وحدة تخزين كاملة لكنها تكون مؤقتة بحيث يستخدمها المستخدم بعد فتح المجلد ثم يغلقها مرة أخرى. يدعم فيراكريبت خوارزميات تشفير متعددة، كما يسمح بإنشاء مجلدات للتمويه، مما يعطي المستخدم العديد من الخيارات لتشفير الملفات، ولا يقتصر استخدام فيراكريبت على الملفات المتواجدة على جهاز الحاسب، بل يمكن من خلاله أيضا تشفير أجهزة التخزين بالكامل بالإضافة إلى وحدات التخزين في القرص الصلب. يوصَى بتحميل البرنامج من موقعه الرسمي واختيار الحزمة حسب نظام التشغيل المستخدم

استخدامه على نظام ويندوز

يوفر فيراكريبت لنظام ويندوز خيارين لاستخدامه؛ الأول هو تنصيب البرنامج على النظام، والثاني هو استخدام النسخة المحمولة دون تنصيب البرنامج. ويمكن للمستخدم اختيار الحزمة الأنسب عبر تحديد طبيعة استخدامه للبرنامج، فإذا كان يعتزم استخدامه على جهازه الخاص ولا مانع لديه من ظهوره في قائمة البرامج المثبتة يمكنه اختيار إحدى حزم تنصيب البرنامج (EXE Installer أو MSI Installer)، أما إذا كان يعتزم حمله في وحدة تخزين خارجية واستخدامه على أجهزة متعددة فيحتاج استخدامه سريعا دون الحاجة إلى تنصيبه كل مرة أو إذا لم يكن يريد ظهور البرنامج في قائمة البرامج المثبتة يمكنه اختيار النسخة المحمولة (Portable version) والتي تتميز بعدم الحاجة إلى صلاحيات إدارية لاستخدامها.

استخدامه على نظام لينكس

يوفر الموقع الرسمي حزم تنصيب لعدد من توزيعات لينكس الشهيرة، كما يوفر الكود المصدري لبناء البرنامج على أي توزيعة إذا لم تكن هناك حزمة تنصيب جاهزة متوفرة للتوزيعة التي يستخدمها المستخدم. لا توجد نسخة محمولة من فيراكريبت بشكل رسمي على أنظمة لينكس، ويأتي البرنامج على أنظمة لينكس في صورتين؛ الأولى هي الواجهة الرسومية الشبيهة بنسخة البرنامج للأنظمة الأخرى، والثانية هي نسخة سطر الأوامر.

استخدامه على نظام macOS

يجب تنصيب macFUSE أولا قبل تنصيب فيراكريبت على macOS، ويمكن إيجاد رابط macFUSE في صفحة تحميلات فيراكريبت تحت اسم OSXFUSE، وبعد تنصيبه يمكن تنصيب فيراكريبت إذا كانت نسخة نظام macOS هي 10.9 أو أحدث، ولا تتوفر نسخة محمولة من فيراكريبت على نظام macOS.

استخدامه على نظام أندرويد

لا يدعم فيراكريبت أنظمة تشغيل الهاتف لكن يمكن استخدام تطبيقات أخرى مثل EDS Lite لفتح بعض الحاويات التي تم إنشاؤها باستخدام فيراكريبت على هواتف أندرويد، مع

ملاحظة أن هذا التطبيق به مزايا محدودة جدا ولا يوصى بالاعتماد عليه تماما بسبب محدوديته وعدم حصوله على تحديثات دورية.

استخدام فيراكريبت بعد تنصيبه

يتمكن المستخدم عبر استخدام فيراكريبت من تشفير أنواع مختلفة من مساحات التخزين، وسنشرح هنا إنشاء مجلدات مشفرة اعتيادية للملفات وفتحها عند الحاجة، وتلك هي الخطوات لإنشاء مجلد مشفر قياسي في ملف:

1. إنشاء المجلد المشفر

بعد فتح البرنامج، عند الضغط على `Create Volume` تظهر نافذة يمكن اختيار `Create an encrypted file container` منها، ثم الضغط على `Next`. وفي النافذة التالية يمكن اختيار `Standard VeraCrypt Container` ثم الضغط على `Next`. وفي النافذة التالية يمكن الضغط على `Select File` واختيار اسم الملف الذي نريد إنشاؤه حتى يحتوي المجلد المشفر، وبعد اختيار مكان الملف واسمه يمكن الضغط على `Next`، ويجب تجنب اختيار ملفات مهمة موجودة بالفعل فهذا لن يقوم بتشفير تلك الملفات إنما سيقوم بمحوها واستبدالها بالمجلد المشفر. وفي النافذة التالية يمكن الضغط على `Next`. وفي النافذة التالية يمكن اختيار حجم المجلد عبر كتابة رقم ثم اختيار الوحدة (فمثلا إذا رغب المستخدم بإنشاء مجلد يتسع لاستيعاب ملفات تصل إلى 5 جيجابايت، يكتب رقم 5 ويختار وحدة `GB`) ثم الضغط على `Next`. وفي النافذة التالية يمكن كتابة كلمة السر لفك تشفير المجلد وتأكيدها مرة أخرى ثم الضغط على `Next`. وفي النافذة التالية يوصى بتحريك الفأرة عشوائيا بداخل النافذة لبعض الوقت ثم الضغط على `Format` وانتظار البرنامج حتى ينتهي من إنشاء المجلد، وبعد الانتهاء من إنشاء المجلد يمكن الضغط على `OK` والخروج من النافذة عبر الضغط على `Exit`.

2. استخدام المجلد المشفر

بعد فتح البرنامج يمكن فتح مجلد مشفر تم إنشاؤه مسبقا عبر الضغط على أي حرف أو رقم من الخيارات الكثيرة المتاحة في خانة Drive أو Slot ثم الضغط على `Select File...` واختيار الملف الذي يحتوي المجلد المشفر، ثم الضغط على `Mount`، ثم كتابة

كلمة المرور التي تم اختيارها عند إنشاء ذلك المجلد، ثم الضغط على `OK`، وإذا كانت كلمة المرور صحيحة، سيقوم فيراكريبت بفك تشفير المجلد وسيظهر في شكل وحدة تخزين على جهاز الكمبيوتر يمكن نقل الملفات إليها أو منها أو إنشاء وتعديل الملفات بداخلها، وبعد الانتهاء من استخدام المجلد يمكن إغلاقه مجددا عبر فتح فيراكريبت وتحديد المجلد والضغط على `Dismount`.

لإضافة وسيلة تمويه بسيطة يمكن تغيير اسم الملف الذي يحتوي على المجلد بحيث تدل لاحقة الملف على نوع معين من الملفات، كلاحقة mp4 لملفات الفيديو مثلا، وهو ما سيجعل الملف يبدو من الخارج بذلك النوع وعند محاولة فتحه دون فك التشفير سيحاول مشغل الفيديو فتحه لكنه لن يصبح قادرا على تشغيله.

Picocrypt

لا يقوم بيكوكريبت بتشفير أقراص كاملة أو أجهزة تخزين، فعمله يقتصر على تشفير الملفات والمجلدات، وهو يعمل على أنظمة تشغيل الحاسب مثل ويندوز ولينكس وmacOS مع وجود نسخة بدائية منه تعمل على الويب مباشرة، ويتميز بعدم حاجته إلى صلاحيات إدارية للعمل وقدرته على العمل دون تنصيب وحجمه الصغير والسهولة النسبية لاستخدامه بالإضافة إلى خيارات الأمان التي يقدمها، ولا يعتزم مطوروا البرنامج إضافة خصائص جديدة لتجنب الثغرات المحتملة مع الخصائص الجديدة، ويوصى بتحميله من صفحته على موقع GitHub واختيار الحزمة الملائمة لنظام التشغيل الذي سيتم استخدامه عليه.

تحميله على نظام ويندوز

يوفر بيكوكريبت لنظام ويندوز خيارين لاستخدامه؛ الأول هو تنصيب البرنامج على النظام، والثاني هو استخدام النسخة المحمولة دون تنصيب البرنامج. ويمكن للمستخدم اختيار الحزمة الأنسب عبر تحديد طبيعة استخدامه للبرنامج، فإذا كان يعتزم استخدامه على جهازه الخاص ولا مانع لديه من ظهوره في قائمة البرامج المثبتة يمكنه اختيار حزمة Installer.exe

لتنصيب البرنامج، أما إذا كان يعتزم حمله في وحدة تخزين خارجية واستخدامه على أجهزة متعددة فيحتاج استخدامه سريعا دون الحاجة إلى تنصيبه كل مرة أو إذا لم يكن يريد ظهور البرنامج في قائمة البرامج المثبتة يمكنه اختيار النسخة المحمولة لنظام ويندوز Picocrypt.exe والتي تتميز بعدم الحاجة إلى صلاحيات إدارية لاستخدامها.

تحميله على أنظمة لينكس

الطريقة الأولى لاستخدام بيكوكريبت على أنظمة لينكس هي حزمة appimage المتوفرة في صفحة التحميلات باسم Picocrypt.AppImage والتي تعتبر نسخة محمولة تعمل على معظم التوزيعات دون الحاجة إلى التنصيب ويمكن حملها في وحدة تخزين خارجية واستخدامها على أجهزة متعددة دون الحاجة إلى تنصيب البرنامج كل مرة، ولطريقة أخرى يمكن تنصيب البرنامج عبر حزمة snap المتوفرة على متجر سناب. ويمكن كذلك استخدام الكود المصدري لبناء البرنامج باستخدام الإرشادات الموجودة على صفحة البرنامج على موقع GitHub.

تحميله على نظام macOS

لاستخدام بيكوكريبت على ماك أو إس يوصى بتحميل حزمة Picocrypt.app.zip والقيام بفك ضغطها وتشغيل بيكوكريبت الموجود بداخلها.

استخدامه على الويب

يوفر بيكوكريبت نسخة بدائية من البرنامج على الويب ولا تحتوي تلك النسخة سوى على إمكانية التشفير وفكه بشكل أساسي دون دعم المزايا الأخرى الموجودة في نسخ سطح المكتب من البرنامج، وتسمح نسخة الويب من بيكوكريبت باستخدامه على الهواتف دون الحاجة إلى تنصيب تطبيق جديد، وتتوفر نسخة الويب على الموقع:
https://picocrypt.pages.dev

استخدام بيكوكريبت بعد تحميله

يمكن تشفير الملفات أو المجلدات باستخدام بيكوكريبت عبر سحبها إلى نافذة البرنامج وإفلاتها بداخلها، ثم اختيار كلمة السر وتأكيدها مرة أخرى، والضغط على Encrypt، وسيقوم

البرنامج بصنع ملف مشفر يمكن استخدامه فيما بعد لفك تشفير تلك الملفات أو المجلدات. ويمكن فك تشفير الملفات التي صُنعت بواسطة نفس البرنامج عبر سحبها إلى نافذة البرنامج وإفلاتها بداخلها، ثم كتابة كلمة السر التي تم اختيارها عند القيام بالتشفير، ثم الضغط على Decrypt وسيقوم البرنامج بفك التشفير واستخراج نسخة غير مشفرة لاستخدامها.

خيارات التشفير

1. توليد كلمات السر

يحتوي بيكوكريبت بداخله على أداة لتوليد كلمات السر عند الرغبة في توليد كلمات سر قوية، ويمكن الوصول إلى هذه الأداة أثناء القيام بعملية التشفير، فبعد سحب الملفات أو المجلدات وإفلاتها داخل نافذة البرنامج يمكن الضغط على زر Create واختيار عدد محارف كلمة السر ونوع تلك المحارف وما إذا كان البرنامج سينسخ كلمة السر إلى الحافظة للصقها في أي مكان آخر مثل مدير كلمات السر.

2. الملفات المفتاحية

يسمح بيكوكريبت باستخدام ملفات مفتاحية (keyfiles) إلى جانب كلمات السر أو عوضا عنها، بمعنى أن يشترط البرنامج وجود ملف معين يشير إليه المستخدم حتى يتمكن من القيام بفك التشفير، ويصبح خيار استخدام الملفات المفتاحية متاحا في جزء keyfiles بعد سحب وإفلات الملفات أو المجلدات إلى نافذة البرنامج، وفي حالة الرغبة في استخدام أي ملفات متواجدة بالفعل يمكن الضغط على edit ثم سحب وإفلات الملف (أو مجموعة من الملفات) داخل نافذة البرنامج، وهنا يصبح خيار Require correct order متاحا، وتفعيله يعني أن استخدام الملفات المفتاحية في عملية فك التشفير لا بد من أن يكون بنفس ترتيب الملفات الذي كان عليه في عملية التشفير، ثم الضغط على done لاعتماد الملفات المفتاحية مفتاحا لفك التشفير.

3. الملحوظات

يمكن إضافة ملحوظات إلى الملف المشفر تظهر عند سحب الملف المشفر وإفلاته في نافذة بيكوكريبت قبل فك التشفير، ولا يتم تشفير تلك الملحوظات، لذلك لا يجب استخدامها للإشارة إلى معلومات حساسة.

4. وضع الذعر

عند تشفير الملفات أو المجلدات، يمكن تحديد خيار Paranoid mode (وضع الذعر)، وعند تفعيله يقوم البرنامج برفع درجة تعقيد التشفير واستخدام المزيد من طبقات الحماية. ولا يعتبر هذا الخيار ضروريا سوى عند الشك باحتمال قيام أجهزة ذات إمكانات وموارد هائلة بمحاولة فك التشفير. وعند تفعيل هذا الخيارقد تكون عملية التشفير وفكه أبطأ.

5. ضغط الملفات

لا يقوم بيكوكريبت افتراضيا بضغط الملفات عند تشفيرها لكنه يتيح ذلك الخيار عبر الضغط على Compress files أثناء إعداد التشفير فيقوم بيكوكريبت عند تفعيل هذا الخيار بضغط الملفات أثناء التشفير باستخدام خوارزمية ديفليت وقد يزيد هذا الخيار من بطء عمليتي التشفير وفك التشفير قليلا.

6. تصحيح الخطأ

عند الرغبة في تخزين الملفات المشفرة لوقت طويل على أقراص قد تتعرض للتلف أو عند القلق من تلف الملفات عند تخزينها على الخدمات السحابية يمكن تفعيل مصحح الخطأ Reed-Solomon، وهو يقوم باستخدام كود ريد-سولومون في الملف المشفر حتى يمكن فك تشفيره حتى إذا تعرض الملف إلى تلف يصل إلى 3% من حجمه، أما إذا كان حجم التلف يتجاوز هذه النسبية فسيحاول البرنامج استرداد ما يتمكن من استرداده، ولكن تقوم تلك الخاصية بإبطاء سرعتي التشفير وفك التشفير بشكل ملحوظ.

7. محو الملفات

عند القيام بتشفير ملفات أو مجلدات باستخدام بيكوكريبت فإنه يقوم بإنشاء نسخة مشفرة من تلك الملفات أو المجلدات فقط، لكن يمكن كذلك عند القيام بالتشفير تفعيل خيار Delete files والذي سيقوم بمحو الملفات أو المجلدات الأصلية غير المشفرة بعد القيام بتشفيرها حتى لا تتواجد سوى النسخة المشفرة.

8. القدرة على الإنكار

يحمل الملف المشفر بواسطة بيكوكريبت لاحقة (pcv) في نهاية اسم الملف، ولكن يمكن للمستخدمين تغييرها يدويا إلى أي لاحقة أخرى لإخفاء طبيعة الملف (أن يبدل اسم الملف File.pcv إلى File.mp4 وهو ما سيجعل الملف يبدو ملف فيديو بين الملفات الأخرى من الخارج) لكن يجب بعد ذلك إعادة وضع تلك اللاحقة في اسم الملف عند الرغبة في فك تشفيره، وتوفر تلك الطريقة تخفيا بسيطا لكن يمكن لمن لديه المعرفة التقنية استنتاج طبيعة

الملف الحقيقية (كونه ملفا مشفرا من إنشاء بيكوكريبت) عبر فحص بياناته، وعند القلق من فحص الملفات فحصا دقيقا بواسطة أشخاص ذوي معرفة تقنية واسعة، يمكن تفعيل خيار Deniability عند القيام بتشفير الملفات أو المجلدات فيقوم بيكوكريبت بإجراء تغييرات على تسلسل بيانات الملف تجعل منه ملفا لا يمكن استنتاج طبيعته الحقيقية حتى من خلال فحصه بواسطة خبراء، لكن لا يزال على المستخدم أيضا القيام بتغيير اسم الملف يدويا، ويؤدي تفعيل هذا الخيار إلى إبطاء عمليتي التشفير وفك التشفير وإلغاء مزايا وضع الذعر وإتلاف الملحوظات.

9. التقسيم إلى أجزاء

مهما كان عدد الملفات أو المجلدات التي يتم تشفيرها باستخدام بيكوكريبت فإنه ينتج ملفا مشفرا واحدا في كل عملية تشفير، لكن البرنامج يوفر خيارا لتقسيم ذلك الملف إلى أجزاء أصغر حتى يسهل رفعها على خدمات التخزين السحابي أو لتوزيعها بين أشخاص مختلفين فيصبح تواجد جميع الأجزاء ضروريا لفك التشفير، ويمكن تفعيل ذلك الخيار عبر الضغط على Split into chunks واختيار حجم الأجزاء ووحدة الحجم، فمثلا إذا قام مستخدم بتشفير ملف حجمه 10 ميجابايت واختار تقسيمه إلى أجزاء بحجم 1 ميجابايت سينتج عن هذا 10 أجزاء مشفرة حجم كل منها 1 ميجابايت، أو يمكن اختيار عدد الملفات المرجو تقسيم الملف المشفر إليه عبر اختيار Total في وحدة الحجم. ويكفي عند فك التشفير أن يتم سحب واحد من تلك الأجزاء وإفلاته في نافذة البرنامج حتى يقوم بجمع الأجزاء الأخرى شرط أن تكون في نفس المجلد وأن تحمل نفس النهايات الموضوعة عند التشفير.

خيارات فك التشفير

1. الإجبار على فك التشفير

عند القيام بفك تشفير أحد الملفات التي تم إنشاؤها بواسطة بيكوكريبت، يقوم البرنامج أولا بفحص الملف المشفر للتأكد من عدم تعرضه للتلاعب أو التعديل، وإذا عثر على تلاعب أو تلف في الملف يقوم بمحو الملف الناتج، لكن عند رغبة المستخدم بتجاوز ذلك الإجراء يمكنه تفعيل خيار Force decrypt عند القيام بفك تشفير الملف، ويكون هذا الخيار مفيدا عند تعرض الملف للتلف البسيط إذا كان خيار تصحيح الخطأ باستخدام كود ريد-سولومون مفعلا عند التشفير لأن البرنامج سيحاول استرداد ما يمكن استرداده منه.

2. محو الملف المشفر

عند القيام بفك تشفير أحد الملفات التي تم إنشاؤها بواسطة بيكوكريبت فإنه يعيد إنشاء نسخة غير مشفرة من تلك الملفات أو المجلدات مع الحفاظ على الملف المشفر، لكن يمكن كذلك عند القيام بفك التشفير تفعيل خيار Delete volume والذي سيقوم بمحو الملف المشفر والإبقاء على الملفات التي تم فك تشفيرها عند عدم الحاجة إلى النسخة المشفرة بعد فك التشفير.

ثانيا: الهواتف

Tella

يهدف تيلا بشكل أساسي إلى مساعدة الصحفيين في توثيق البيانات والأحداث بسرية والاحتفاظ بها مشفرة والتخلص منها بسرعة إذا استدعت الحاجة، ويعمل التطبيق على نظامي أندرويد وiOS ويمكن استخدامه عموما بواسطة أي شخص بهدف الاحتفاظ بالبيانات مشفرة على الهاتف. يوفر تيلا عدة مميزات تتضمن إنشاء المحتوى داخل التطبيق كالتقاط الصور ومقاطع الفيديو والتسجيلات الصوتية وسبل للتمويه كتغيير أيقونة التطبيق (على أندرويد فقط) وإمكانية توصيله بسيرفر عبر الإنترنت لمزامنة المحتويات.

تحميله على أندرويد

توجد نسختان من تطبيق تيلا لأندرويد؛ الأولى هي النسخة الأساسية وهي متوفرة على متجر تطبيقات بلاي والثانية هي النسخة مفتوحة المصدر بالكامل، ورغم أن النسخة الأساسية مفتوحة المصدر إلا أنها تعتمد في بعض مكوناتها على برمجيات أخرى غير مفتوحة المصدر، ولذلك تتوفر نسخة أخرى لا توجد بها أي مكونات غير مفتوحة المصدر ويمكن

تحميلها من F-droid لكن يجب العلم أنها أقل في المزايا من النسخة الأساسية فهي مثلا لا تدعم خدمة Tella web حتى الآن.

تحميله على أيفون

يمكن تحميل تيلا على هواتف iPhone من متجر التطبيقات الرسمي ولا زالت نسخة iOS متأخرة قليلا في بعض المزايا عن نسخة نظام أندرويد الأساسية كما يقيد نظام iOS من بعض المزايا فهو لا يسمح مثلا بتغيير أيقونة التطبيق كما هو ممكن على نظام أندرويد.

استخدام تيلا

1. قفل التطبيق

لبدء استخدام التطبيق على المستخدم اختيار طريقة لقفله ولن يتمكن أي شخص من الوصول إلى محتويات التطبيق دون معرفة وسيلة قفله، ويوفر تيلا ثلاثة خيارات لقفل التطبيق؛ الأول هو استخدام كلمة مرور، ويعتبر هذا الخيار الأكثر أمانا خاصة إذا ما كان عدد حروف كلمة المرور أطول من 14 وكانت معقدة باحتوائها على حروف صغيرة وكبيرة وأرقام ورموز، والخيار الثاني لقفل التطبيق هو رمز التعريف الشخصي، وهو خيار أقل أمانا من كلمة المرور لكنه قد يكون أسهل بالنسبة للبعض، والخيار الثالث هي النمط، ويعتبر هذا الخيار أقل الخيارات أمانا بين الثلاثة كما أنه ليس متوفرا على نظام iOS. ويجب أن يتأكد المستخدم من قدرته على تذكر وسيلة دخوله للتطبيق حيث لا توجد طريقة لاستعادة الملفات في حالة نسيان كلمة المرور أو رمز التعريف الشخصي أو النمط، وسيضطر المستخدم إلى حذف التطبيق وتثبيته مرة أخرى (أو حذف بياناته) حتى يتمكن من استخدامه مجددا وسيخسر كل ما كان مخزنا بداخل التطبيق.

لاستخدام التطبيق لا بد للمستخدم من تقديم وسيلة فتح التطبيق، ويقوم التطبيق بإغلاق المحتويات مجددا بمجرد خروج المستخدم من التطبيق أو قفل الشاشة، لكن يمكن التحكم في فترة الانتظار قبل قفل التطبيق عبر فتح إعدادات التطبيق واختيار الأمان وتغيير الوقت المخصص لتفعيل قفل التأمين بواحد من خيارات المدة الزمنية قبل قفل التطبيق.

2. إدارة الملفات

يوفر تطبيق تيلا بداخله إمكانية تصفح الملفات وإدارتها عبر تقسيم الملفات المتاحة داخله إلى أنواعها المختلفة بالإضافة إلى إمكانية تصفح جميع الملفات وإنشاء المجلدات وترتيب الملفات بداخلها. عند التقاط صور أو مقاطع فيديو أو تسجيل مقاطع صوتية داخل التطبيق يقوم تيلا بتشفيرها والاحتفاظ بها داخله ويمكن تصفحها داخل التطبيق فقط، لكن يمكن تصدير أي ملف بواسطة المستخدم خارج التطبيق لاستخدامه في أي شيء آخر لكن تصدير الملفات خارج التطبيق يعني أنها لا تصبح مشفرة، ويمكن القيام بالعكس كذلك عبر استيراد الملفات من خارج تيلا إلى داخله حتى تصير تلك الملفات مشفرة، وتقتصر إمكانية تصفح الملفات داخل تطبيق تيلا على الصور ومقاطع الفيديو والتسجيلات الصوتية في نسختي أندرويد، وتقتصر على الصور ومقاطع الفيديو والتسجيلات الصوتية بالإضافة إلى ملفات PDF في نسخة التطبيق لنظام iOS.

عند استيراد الملفات داخل التطبيق في نسخة أندرويد الأساسية وفي نسخة iOS يمكن للمستخدم أن يقرر ما إذا كان يريد حذف الملف الأصلي الموجود خارج التطبيق أو لا، ولا تتوفر تلك الميزة في النسخة مفتوحة المصدر بالكامل حتى الآن، وإذا قرر المستخدم عدم حذف الملف الأصلي ستصبح نسختان من الملف متوفرتان؛ إحداهما مشفرة داخل التطبيق والأخرى غير مشفرة خارج التطبيق. ويتوفر في نسخة أندرويد الأساسية فقط خيار الحفاظ على البيانات الوصفية للملفات عند استيرادها من الجهاز.

3. التمويه

ليس التمويه مدعوما سوى في نسختي أندرويد وهو غير ممكن في نظام iOS ويوجد خياران أساسيان للتمويه في تطبيق تيلا؛ الأول هو تغيير الاسم والأيقونة، والثاني هو الإخفاء خلف تطبيق آلة حاسبة. في الخيار الأول يمكن للمستخدم اختيار أيقونه واسما مختلفين ضمن خيارات محددة متوفرة في التطبيق ليظهر التطبيق بالاسم والأيقونة الذين تم اختيارهما في الشاشة الرئيسية عوضا عن اسم وأيقونة تطبيق تيلا، وفي الخيار الآخر يتحول تطبيق تيلا إلى تطبيق آلة حاسبة فعلي، ويمكن فتح تيلا في هذا الوضع عبر إدخال رقم التعريف الشخصي في الآلة الحاسبة، ولا يعمل هذا الخيار سوى عند اختيار رقم التعريف الشخصي لقفل التطبيق.

4. الوضع الصامت للكاميرا

يسمح تيلا بتفعيل الوضع الصامت للكاميرا حتى يتمكن المستخدم من التقاط الصور ومقاطع الفيديو دون إصدار صوت عند الرغبة في توثيق الأحداث دون لفت الانتباه، وتتوفر هذه الخاصية في نسختي أندرويد (النسخة الأساسية والنسخة مفتوحة المصدر بالكامل)، لكنها ليست متوفرة حتى الآن في نسخة التطبيق لنظام iOS. ويمكن تفعيل هذا الوضع عبر فتح إعدادات التطبيق واختيار الأمان ثم تفعيل خيار الوضع الصامت للكاميرا.

5. أمان الشاشة

يقوم هذا الخيار بوقف إمكانية أخذ لقطات للشاشة أو تسجيل الشاشة داخل التطبيق، كما لا يسمح بظهور صورة معاينة للشاشة في قائمة التطبيقات المفتوحة، ويكون هذا الخيار مفيدا لمنع مشاركة محتوى التطبيق عبر مشاركة الشاشة باستخدام أي تطبيقات أخرى أو عند بث شاشة إلى شاشة خارجية أو جهاز كمبيوتر، وقد يكون هذا الخيار مفعلا تلقائيا، ويمكن التحكم به في إعدادات التطبيق عبر اختيار الأمان ثم تفعيل أو إلغاء خيار Screen security.

6. نمط التحقق

في نسختي التطبيق لنظام أندرويد يمكن تفعيل نمط التحقق عبر دخول أعدادات التطبيق والضغط على عام قم تفعيل خيار نمط التحقق، ويقوم هذا الخيار بجمع عدد من البيانات حول الصور ومقاطع الفيديو والتسجيلات الصوتية من أجل إضافة وسيلة لإثبات بعض البيانات حول تلك الملفات، وتشمل البيانات التي يتم إضافتها للملفات عند تفعيل ذلك الوضع بيانات حول الملف مثل مساره وتاريخ تعديله، وبيانات حول الجهاز مثل الشركة المصنعة والإصدار والرقم التعريفي واللغة المستخدمة وحجم الشاشة وبيانات الشبكة، وأخيرا بيانات حول بيئة إنشاء تلك الملفات مثل البيانات التفصيلية للموقع الجغرافي والشبكة التي كان الهاتف متصلا بها في ذلك الوقت. ويتم إضافة تلك البيانات في ملف منفصل بصيغة csv والتي يمكن فتحها باستخدام برامج جداول البيانات مثل LibreOffice Calc.

7. الحذف السريع

يمكن تفعيل خيار الحذف السريع عند القلق من كشف المعلومات الموجودة بداخله في حال الشعور بالتهديد وفي حالات الطوارئ، ويسمح ذلك الخيار بوجود زر منسدل على شاشة التطبيق الرئيسية لحذف محتويات من التطبيق يحددها المستخدم مسبقا عند تفعيل ذلك

الخيار. ولتفعيل ذلك الخيار يمكن التوجه إلى إعدادات التطبيق والضغط على الأمان وتفعيل خيار الحذف السريع ثم تحديد البيانات التي يجب حذفها عند سحب ذلك الزر. وتوجد أربعة خيارات لما يمكن حذفه عند سحب زر الحذف السريع.

1. احذف المخزن: عند تحديد ذلك الخيار يقوم التطبيق بحذف جميع الملفات المخزنة داخل التطبيق.
2. حذف مسودات النماذج والنماذج المقدمة
3. حذف إعدادات الخادم: عند تحديد ذلك الخيار يقوم التطبيق بحذف بيانات الاتصال بالخوادم وجميع النماذج المرتبطة بها.
4. حذف Tella: عند تفعيل ذلك الخيار يتم حذف التطبيق بالكامل بما يتضمن جميع البيانات المحفوظة بداخله، وذلك عن طريق عرض خيار لإزالة تثبيت التطبيق التي يجب الموافقة عليها حتى يتم حذف جميع تلك البيانات.

8. الخوادم

إذا كان المستخدم عضوا في مجموعة أو منظمة تمتلك خادما يمكن استخدامه لإرسال البيانات والملفات، يمكنه الاتصال بهذا الخادم عبر تطبيق تيلا، ويؤدي الاتصال بالخوادم إلى رفع نسخ احتياطية من الملفات إلى الخادم لضمان عدم ضياعها، ويدعم تيلا ثلاثة أنواع من الخوادم هي تيلا وِب (Tella Web) وأوبن داتا كِت (ODK) وأوازي (Uwazi).

الفرق بين نسخ التطبيق المختلفة

تتشابه النسخ الثلاثة من تطبيق تيلا في الشكل وطريقة الاستخدام، لكنها تختلف عن بعضها في أشياء طفيفة:

	نسخة أندرويد الأساسية	نسخة أندرويد مفتوحة المصدر	نسخة iOS
طرق قفل التطبيق	- كلمة مرور - رمز تعريف شخصي - نمط	- كلمة مرور - رمز تعريف شخصي - نمط	- كلمة مرور - رمز تعريف شخصي
كتم صوت الكاميرا	متوفر	متوفر	ليس متوفرا حتى الآن

	نسخة أندرويد الأساسية	نسخة أندرويد مفتوحة المصدر	نسخة iOS
استيراد الملفات من خارج تيلا	متوفر	متوفر دون حذف الملف الأصلي	متوفر
استيراد بالبيانات الوصفية	متوفر	ليس متوفرا حتى الآن	ليس متوفرا حتى الآن
التمويه	متوفر	متوفر	غير ممكن في iOS
التصوير داخل التطبيق	متوفر	متوفر مع نقص بعض الخصائص	متوفر
تحديد دقة الفيديو	متوفر	ليس متوفرا حتى الآن	ليس متوفرا حتى الآن
الملفات التي يمكن فتحها داخل تيلا	الصور ومقاطع الفيديو وتسجيلات الصوت	الصور ومقاطع الفيديو وتسجيلات الصوت	الصور ومقاطع الفيديو وتسجيلات الصوت وملفات PDF
نمط التحقق	متوفر	متوفر	ليس متوفرا حتى الآن

DroidFS

يعمل DroidFS على نظام أندرويد عبر إنشاء مجلدات مشفرة خارج التطبيق أو داخله لحفظ الملفات داخلها بشكل آمن، ويتطلب فك تشفير تلك المجلدات إدخال كلمة المرور التي سبق اختيارها عند إنشاء المجلد، ويتوافق DroidFS مع برمجيات تشفير أخرى ويعتمد عليها مثل Gocryptfs و CryFS، ويمكّن المستخدم من إنشاء نوعين من المجلدات المشفرة؛ أحدهما مجلد خارجي تظل بياناته على ذاكرة الجهاز منفصلة عن بيانات التطبيق، والآخر مجلد مخفي داخل الجهاز متضمن في بيانات التطبيق.

تحميله

لا يتوفر DroidFS للتحميل عبر متجر تطبيقات جوجل بلاي حتى الآن، لكن يمكن تحميله من خلال متجر تطبيقات F-Droid، ويمكن كذلك تحميله من خلال صفحة التطبيق على موقع Chapril أو من خلال صفحة التطبيق على موقع GitHub، ويوفر مطورو التطبيق كذلك توقيعات PGP للتحقق من نزاهة الحزمة المتوفرة للتنزل عبر هذين الموقعين.

استخدامه

يمكن استخدام DroidFS كأداة لصنع المجلدات المشفرة وكذلك لتصفح محتويات تلك المجلدات، فهو يحتوى على مدير للملفات لعرض والتحكم في محتويات المجلدات المشفرة، ويتيح التطبيق عدة خيارات للتحكم في مستوى الأمان وطرق عرض الملفات ويوفر خيارات لا يرشحها بشكل افتراضي لكن يمكن للمستخدم تفعيلها عند الحاجة إليها، ويمكن بعد فتح مجلد مشفر إنشاء الملفات داخل التطبيق واستيراد الملفات والمجلدات من ذاكرة الجهاز لحفظها بشكل مشفر داخل المجلد المشفر، ويمكن أيضا التقاط الصور ومقاطع الفيديو داخل التطبيق ليتم حفظ تلك الصور ومقاطع الفيديو داخل المجلد المشفر مباشرة.

1. إنشاء مجلد مشفر

بعد فتح التطبيق يمكن الضغط على زر + لإنشاء مجلد مشفر (ويستخدم نفس الزر أيضا لفتح المجلدات المشفرة الموجودة بالفعل)، ثم يقوم المستخدم بتحديد ما إذا كان يريد المجلد المشفر مخفيا أم لا، وهناك فرق في ظهور ومكان تخزين المجلد المشفر بين هذين الخيارين.

- **مجلد مشفر مخفي**: يتم تخزين هذا المجلد المشفر ضمن بيانات تطبيق DroidFS وهذا يعني عدم تواجده بشكل ظاهر في الملفات الخارجية على الجهاز ولا يمكن للتطبيقات الأخرى رؤيته دون صلاحيات الجذر (root)، ولكن يتوقف الحفاظ على ذلك المجلد بالحفاظ على بيانات التطبيق، أي إذا تعرض التطبيق للحذف أو محو البيانات يتم محو المجلد المشفر كذلك لهذا يجب التأكد من النسخ الاحتياطي لبيانات التطبيق بالكامل للحفاظ على محتويات المجلد المشفر المخفي من الضياع، ويتم إنشاؤه عبر تعيين اسم له يجب تذكره عند الرغبة في فتح المجلد.
- **مجلد مشفر غير مخفي**: يتم تخزين هذا المجلد المشفر خارج بيانات تطبيق DroidFS وهذا يعني وجوده على هيئة بيانات مشفرة توجد في مكان يختاره المستخدم، ولا يرتبط ذلك المجلد المشفر بتطبيق DroidFS فهو منفصل في تخزينه عن التطبيق، ويمكن لأي تطبيق له وصول لملفات الجهاز من رؤية تلك الملفات (بشكلها المشفر، وليس الوصول إلى المحتوى الموجود بداخل المجلد) ويمكن نسخ المجلد المشفر غير المخفي احتياطيا والحفاظ عليه عبر النسخ الاحتياطي لهذه الملفات الظاهرة، وهو ما يساعد المستخدم في الوصول إليها مجددا حتى إذا تم حذف تطبيق DroidFS أو محو بياناته.

بعد تعيين اسم المجلد للمجلدات المشفرة المخفية أو اختيار مسار المجلد للمجلدات غير المخفية يضغط المستخدم على زر **إنشاء مجلد مشفر** ثم يتعين عليه في الصفحة التالية اختيار كلمة مرور وتأكيدها ثم الضغط على إنشاء، وبهذا يصبح المجلد المشفر جاهزا للاستخدام.

2. فتح مجلد مشفر

يمكن فتح المجلدات المشفرة عبر الضغط على زر +، ثم تحديد ما إذا كان المجلد المشفر مخفيا أم لا، ثم تحديد مساره إذا لم يكن مخفيا أو كتابة اسمه إذا كان مخفيا، وبعد ذلك يقوم

المستخدم بإدخال كلمة سر المجلد المشفر وإذا كانت صحيحة يصبح المجلد المشفر جاهزا للاستخدام داخل التطبيق.

الميزات غير الآمنة

يوفر DroidFS ميزات محددة تكون معطلة بشكل تلقائي لكنه يمنح المستخدم حرية تفعيلها إذا كانت هناك حاجة لها، ويمكن الوصول إلى تلك الإعدادات عبر الضغط على أيقونة الترس لفتح إعدادات التطبيق ثم اختيار **إدارة الميزات غير الآمنة**.

1. السماح بلقطة الشاشة

يكون خيار اتخاذ لقطة شاشة داخل تطبيق DroidFS معطلا افتراضيا، وعبر تفعيل خيار **السماح بلقطة الشاشة** يمكن للمستخدم أخذ لقطات للشاشة داخل التطبيق، وهذا يسمح كذلك بظهور محتوى شاشة التطبيق عند تسجيل الشاشة أو بثها إلى شاشة أخرى.

2. السماح بتصدير / فك تشفير الملفات

يحتفظ DroidFS بالملفات داخله ولا يوفر خيار تصديرها أو فك تشفيرها إلى خارج التطبيق بشكل افتراضي، ولتفعيل خيار تصدير الملفات إلى ذاكرة الجهاز في مدير الملفات داخل DroidFS يجب تفعيل خيار **السماح بتصدير / فك تشفير الملفات**، وبهذا يكون من الممكن لأي تطبيق لديه صلاحية الوصول لملفات الجهاز أن يصل إلى تلك الملفات.

3. السماح بفتح الملفات مع التطبيقات الأخرى

يمكن لتطبيق DroidFS استعراض وفتح أنواع محدودة من الملفات، ولهذا قد يحتاج المستخدم إلى فتح الملفات الأخرى باستخدام تطبيقات أخرى، ويمكن تفعيل هذا الخيار في مدير الملفات داخل DroidFS عبر تفعيل خيار **السماح بفتح الملفات مع التطبيقات الأخرى**، وبهذا يمكن فتح الملفات الموجودة داخل المجلد المشفر باستخدام التطبيقات الموجودة على الجهاز ويجب الحذر عند استخدام هذا الخيار لأن بعض التطبيقات قد تقوم بالاحتفاظ بنسخة غير مشفرة من الملف عند فتحه من خلالها.

4. السماح بمشاركة الملفات عبر قائمة المشاركة

يعطل تطبيق DroidFS خيار مشاركة الملفات عبر قائمة الملفات بشكل تلقائي، ويمكن تفعيل هذا الخيار في مدير الملفات داخل DroidFS عبر تفعيل خيار **السماح بمشاركة الملفات عبر قائمة المشاركة**، وبهذا يمكن مشاركة الملفات الموجودة داخل المجلد المشفر باستخدام التطبيقات الموجودة على الجهاز التي تدعم مشاركة كل نوع من تلك الملفات ويجب الحذر عند استخدام هذا الخيار لأنه عبر مشاركة الملفات من خلال تطبيقات أخرى تتمكن تلك التطبيقات أو الأطراف التي تستقبل هذه الملفات بالاحتفاظ بنسخ غير مشفرة من الملفات.

5. إبقاء مجلد التشفير مفتوحا عند الخروج من التطبيق

يغلق تطبيق DroidFS المجلدات المشفرة بمجرد الخروج من التطبيق لحمايتها من وصول أطراف غير مرغوب فيها إلى محتوى تلك المجلدات، لكن إذا أراد المستخدم استخدام محتويات المجلدات المشفرة مع تنقله بين تطبيق DroidFS والتطبيقات الأخرى يمكنه تفعيل خيار **إبقاء مجلد التشفير مفتوحا عند الخروج من التطبيق**، وبهذا تظل المجلدات المشفرة مفتوحة حتى عند الخروج من التطبيق ويحتاج المستخدم إلى قفلها يدويا عند الرغبة بذلك.

6. السماح بحفظ تجزئة كلمة المرور باستخدام بصمة الإصبع

إذا كان المستخدم يستخدم بصمة الإصبع في جهازه يمكنه تفعيل خيار **السماح بحفظ تجزئة كلمة المرور باستخدام بصمة الإصبع**، وسيقوم ذلك الخيار بإنشاء مفتاح AES-256 GCM في مخزن مفاتيح أندرويد المحمي ببصمة الإصبع واستخدامه لتشفير كلمة مرور المجلد المشفر والاحتفاظ به في البيانات الداخلية للتطبيق، ويجب الحذر عند تفعيل ذلك الخيار، فإذا لم يكن الجهاز مشفرا يمكن لمن لديه وصول مادي إلى الجهاز استخراج مفتاح التشفير منه.

ثالثا: أدوات أخرى

توجد العديد من أدوات التشفير الأخرى كالأدوات التي تعمل على سطر الأوامر والأدوات التي تعمل على الويب، ومن الأدوات الجيدة التي تعمل على الويب تطبيق Hat.sh بالإضافة إلى نسخة الويب من تطبيق بيكوكريبت الذي تحدثنا عنه سابقا.

Hat.sh

يعمل Hat.sh كتطبيق ويب على المتصفحات الشهيرة دون قيود مرتبطة بنظام التشغيل، ولا تحتوي خيارات عديدة، إنما تركز على البساطة والسهولة، ويمكن استضافة البرمجية على أي سيرفر أو حتى استخدامها دون اتصال بالإنترنت في حالة الاستضافة الذاتية. يتميز التطبيق بعمله داخل المتصفح دون رفع أي ملفات أو بيانات إلى الموقع مما يجعله أداة عملية عند الحاجة إلى تشفير أو فك تشفير ملف دون تنزيل أو تثبيت أي برامج في وجود المتصفح.

استخدامه

يمكن استخدام Hat.sh عبر الموقع الأساسي للتطبيق (hat.sh) أو أي موقع يستضيف تلك البرمجية، ويوجد عنوانان رسميان للبرمجية في الوقت الحالي:

hat.sh

hat.vercel.app

1. التشفير

تنقسم واجهة التطبيق إلى جزئين أساسيين؛ الأول للتشفير (Encryption) والثاني لفك التشفير (Decryption)، وفي جزء التشفير يمكن اختيار الملفات عبر الضغط على Browse Files أو سحب الملفات وإفلاتها في نافذة التطبيق داخل المتصفح ثم الضغط على NEXT، فيطلب التطبيق كلمة المرور التي سيتم استخدامها في فك التشفير ويساعد التطبيق على

إنشاء كلمات مرور أيضا عبر الضغط على الرمز الموجود في جانب حقل كلمة المرور، ويمكن كذلك استخدام المفتاحين العام والخاص بدلا من كلمة المرور (عند إرسال الملفات المشفرة إلى شخص آخر يمكن استخدام المفتاح العام للمستقبل والمفتاح الخاص للمرسل) لتشفير وفك تشفير الملفات عبر التحويل من خيار Password إلى خيار Public key. وبعد اختيار طريقة التحقق يمكن الضغط على NEXT، فيقوم التطبيق بتشفير الملفات وإتاحة النسخة المشفرة للحفظ عبر الضغط على زر ENCRYPTED FILES، وبعد حفظ الملفات المشفرة يعرض التطبيق خيار Copy Password لنسخ كلمة المرور إلى الحافظة إذا كانت تلك طريقة التشفير المختارة في حال أراد المستخدم الاحتفاظ بها بأي طريقة، وخيار Encrypt more files للعودة إلى عملية التشفير مرة أخرى.

لإضافة وسيلة تمويه بسيطة يمكن تغيير اسم الملف الذي يحتوي على الخزنة بحيث تدل لاحقة الملف على نوع معين من الملفات، كلاحقة mp4 لملفات الفيديو مثلا، وهو ما سيجعل الملف يبدو من الخارج بذلك النوع وعند محاولة فتحه دون فك التشفير سيحاول مشغل الفيديو فتحه لكنه لن يصبح قادرا على تشغيله.

قد يفشل التطبيق في تشفير أو فك تشفير الملفات التي يتجاوز حجمها 1 جيجابايت عند استخدام متصفحات الهاتف أو وضع التصفح الخاص في فايرفوكس مثلا.

2. فك التشفير

لفك التشفير يمكن الضغط على زر Decryption بالأعلى للدخول إلى جزء فك التشفير، وهناك يمكن الضغط على زر Browse Files أو سحب الملفات وإفلاتها في نافذة التطبيق داخل المتصفح ثم الضغط على NEXT، فيطلب التطبيق كلمة المرور التي تم استخدامها عند التشفير إذا كانت تلك طريقة التشفير المختارة أو طلب المفتاح العام للمرسل والمفتاح الخاص للمستقبل إذا كانت تلك طريقة التشفير المختارة، وبعد إدخال كلمة المرور أو المفاتيح يمكن الضغط على NEXT، فيقوم التطبيق بفك تشفير الملفات وإتاحة نسخة غير مشفرة من الملفات للحفظ عبر الضغط على زر DECRYPTED FILES، وبعد حفظ الملفات بعد فك تشفيرها يعرض التطبيق خيار Decrypt Other Files لفك تشفير ملفات أخرى.

ختام

لا يقتصر التخزين الآمن للملفات على القيام بتشفيرها، فماذا سنستفيد إذا كانت الملفات مشفرة لكن تعرضت وحدة التخزين للتلف أو قمنا بمحو محتوياتها بالخطأ، إذا تعرضت وحدة التخزين للضياع فسنتسفيد بأن من يعثر عليها لن يتمكن من الوصول إلى ملفاتنا المشفرة، لكن لهذه الأسباب يجب الاحتفاظ بالملفات في مكان آمن، وإذا كانت مهمة فيجب الاحتفاظ دائما بنسخ احتياطية لأن ضياع أو تلف الملفات أمر ممكن جدا، ويرجع لكل شخص تقدير مدى حساسية ملفاته وحجم التهديد الذي يمكن أن ينتج عن تسريبها، وعلى هذا الأساس يمكن اختيار أدوات تشفير بسيطة أو معقدة.

وفي النهاية نرجو للجميع الأمان والسلامة من جميع التهديدات الرقمية والمادية.