

Start Now!
همراه با CD آموزشی

کلید

Data Security امنیت اطلاعات



پاکسازی غیرقابل بازیابی اطلاعات
رمزنگاری فایل های متنی
رمزگذاری روی فایل ها و پوشه ها

ساخت گاوصندوق امنیتی در کامپیوتر
مخفی کردن گاوصندوق در یک فایل دیگر
تبدیل فلش مموری به کلید گاوصندوق

احمد ولی نتاج - رضا خلیلی

www.keid.ir

ہوا الفتح

« مجموعه کتابهای کاربردی کلید »

کلید امنیت اطلاعات

احمد ولی نتاج - رضا خلیلی

انتشارات
کلید
آموزش

سرشناسه	ولی نتاج، احمد، ۱۳۶۷ -
عنوان و نام پدیدآور	کلید امنیت اطلاعات / احمد ولی نتاج، رضا خلیلی.
مشخصات نشر	تهران: کلید آموزش، ۱۳۹۱.
مشخصات ظاهری	۱۰۴ ص: مصور.
فروست	مجموعه کتابهای کاربردی کلید: ۱۰۸ / طراح و مجری مجموعه منصور سجاد
شابک	978-600-274-016-8
وضعیت فهرست نویسی	فیبا
موضوع	کامپیوترها -- ایمنی اطلاعات
موضوع	شبکه های کامپیوتری -- اقدامات تامینی
شناسه افزوده	خلیلی، رضا، ۱۳۶۷ -
رده بندی کنگره	۱۳۹۱ و ۸ / ک۹ / QAY۶/۹
رده بندی دیویی	۰۰۵/۸
شماره کتابشناسی ملی	۲۸۲۹۰۷۲

کلید امنیت اطلاعات

از مجموعه

کلید - ۱۰۸

info@sajadco.com

طراح و مجری مجموعه: منصور سجاد

مدیر تحریریه: احسان مظلومی

مؤلف: احمد ولی نتاج - رضا خلیلی

مدیر تولید و طراح جلد: مهدی سجاد

ناشر: کلید آموزش

شمارگان: ۳۰۰۰ جلد

نوبت چاپ: چاپ اول - مرداد ۱۳۹۱

شابک: ۹۷۸-۶۰۰-۲۷۴-۰۱۶-۸

قیمت: همراه با CD ۳۵۰۰ تومان

مرکز پخش: ۰۲۱-۶۶۴۰۶۰۶۱-۶۶۹۵۳۰۷۳

۰۳۱۱-۲۲۲۳۷۲۵

۰۲۵۱-۷۷۳۵۴۱۱

- کلیه حقوق و حق چاپ متن، طرح روی جلد و عنوان کتاب با نگرش به قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ محفوظ است و متخلفین تحت پیگرد قانونی قرار می گیرند.
- هرگونه استفاده از عنوان این مجموعه که به ثبت رسیده است ممنوع و متخلفین تحت پیگرد قانونی قرار می گیرند.

برای تهیه مجموعه کتابهای کلید می توانید به سایت www.Kelidshop.ir مراجعه کنید.

برنامه‌ریزی، هدایت و نظارت بر مجموعه کتابهای کاربردی

«کلید»

منصور سجاد

مرداد ۱۳۹۱

:

چاپ اول

برای طرح سوالات خود و گفتگو با مؤلفین کتاب می‌توانید به انجمن کلید به آدرس

www.Kelid.ir/Forum

مراجعه کنید.

آموزش کامپیوتر با مجموعه کتابهای کلید

بر اساس نظرسنجی که در سال ۸۱ انجام شد، کتابهای کامپیوتر موجود در ایران با توجه به اینکه اکثراً از متون خارجی ترجمه شده‌اند، با زیرساختار فرهنگی و همچنین امکانات سخت‌افزاری و نرم‌افزاری موجود در ایران هماهنگ نیست. همچنین در مبحث آموزش کمتر کتابی برای مخاطبین مبتدی منتشر شده است، مجموعه کتابهای کلید با هدف رفع این مشکلات تولید شده است. در این مجموعه با نگرش به سیستم نوین آموزش در دنیا، مباحث مختلف به صورت کاملاً کاربردی و قدم به قدم آموزش داده می‌شود و خواننده کتاب مستقیماً با پروژه‌های عملی درگیر می‌شود. به این ترتیب بدون اینکه از حجم اطلاعات ارائه شده وحشت کند با نرم‌افزار یا محیط مورد نظر آشنا شده و به صورت قدم به قدم آن را قبلی او از کامپیوتر در حد یک اپراتور کتاب می‌تواند به نرم‌افزار و به اجرای پروژه‌های کلام در موضوع مورد نظر آنها توانایی عملی آنان مد



کلید ایمیل
پوشه: بول ایمیل
نمبر: نوبسه آموزشی
۱۰۲ صفحه - ۲۵۰ تومان



مشاقان استفاده از وبلاگ می‌توانند به خوبی از این کتاب استفاده کنند. دومین جلد این مجموعه که ناشر قول داده است ۲۰ جلد از آن را کند "کلید ایمیل" نام دارد.



نگاهی به مجموعه کتابهای کاربردی کامپیوتر
کلیدی برای تمام قفل‌ها

است که خواننده را از ترک محتوای نتوان ساخت و در درازمدت باعث رویگردانی وی می‌شود. بسیاری از این کتابها سطح‌بندی نشده‌اند و در نتیجه خواننده مبتدی باید از همان مرجع افراد حرفه‌ای استفاده کرده و با استفاده از خوش و بی‌خوش خود نیازمندی‌های خود را از بین صفحات کتاب استخراج کند بسیاری از این کتابها در حجم بالا تنظیم شده‌اند و در نتیجه هدف دسترسی سریع و آسان که دستاورد قرن جدید است با مشکل مواجه می‌شود. اما اخیراً انتشارات توسعه آموزش با همکاری بخش سجاد دست به کار تولید مجموعه از کتابهای کامپیوتر شده است که از جمله مهمان ویژه‌های آن می‌توان به موضوعی بودن و کمد بودن آنها اشاره کرد که استفاده از آن برای مبتدیان آشناسی چندانی با حوزه کامپیوتر و اینترنت تا آسان می‌سازد. در این مجموعه سعی شده با روشی جدید برای ترویج "نوین" کتابها، بنا تالیف گزینش و ترجمه نئون مناسب به نیاز خوانندگان و کتبه و معایت سایر کتابها را نداشته باشد کتابها به شیوه آموزش گام به گام تدوین شده

احتمالاً برای شما هم پیش آمده است که بخواهید برای خودتان یک وبلاگ بسازید اما پس از آنکه مقدار زیادی از وقت و انرژی خود را هزینه دید اما به نتیجه دلخواه خود دست نیافتید به این می‌رسید که باید روش سنتی آزمون و خطا را تان شروع و آسان نیست کنار گذاشت و در روشی مناسب‌تر برای انجام این کار اقدام احتمالاً اولین و ساده‌ترین روشی که به می‌رسد استفاده از کتابهای آموزشی اینترنت است که امروزه به وفور در دسترس است. کتابهای علم و تکنولوژی به سادگی در می‌یابید که در علوم و فنون پیشترین کتابها به حاسن دارد که بسیاری از آنها و به حساب چندم هم این کتابها نتوانسته‌اند استانداردهای چندین مؤسسه لایزال متعددی داشته کتابها ترجمه‌های متعددی دارند مشکلات



اکسپرس (Express) خود استفاده کنید. فارسی هم آشنا می‌شویم و یاد می‌گیریم. این موارد با خواندن پیدا کنید.

این طور که معلوم است، در مجموع توسط انتشارات توسعه آموزش و با همکاری می‌شود، هدف آموزش قدم به قدم و تصدیق سانی ساده و کاربردی است. کتاب دیگر رسیده "کلید Chat" نام دارد.



فهرست مطالب

پیشگفتار.....	۷
فصل اول : ساخت گاو صندوق امنیتی با نرم‌افزار Steganos Privacy Suit.....	۹
نصب و آشنایی با محیط نرم‌افزار Steganos Security Suit.....	۱۰
ایجاد یک گاو صندوق الکترونیکی (فضای امن) برای ذخیره اطلاعات.....	۱۴
ورود به گاو صندوق و تنظیمات مربوط به آن.....	۲۰
ایجاد پسوردی قوی و مطمئن.....	۲۸
مخفی کردن یک گاو صندوق در قالب یک فایل.....	۳۴
دسترسی به یک گاو صندوق مخفی شده.....	۳۷
تبدیل کردن حافظه فلش به کلیدی برای باز کردن گاو صندوق.....	۴۰
تبدیل حافظه فلش یا CD/DVD به گاو صندوق.....	۴۲
رمزگذاری روی فایل‌ها و پوشه‌ها.....	۴۷
مدیریت پسوردها.....	۵۲
پاکسازی غیرقابل بازیابی اطلاعات.....	۵۹
فصل دوم : جلوگیری از دسترسی به پوشه‌ها با نرم‌افزار Folder Guard.....	۶۳
نصب نرم‌افزار.....	۶۳
تنظیم نوع دسترسی به یک پوشه.....	۷۰
تنظیم نحوه نمایش اطلاعات یک پوشه.....	۷۴
قرار دادن پسورد برای دستیابی به یک پوشه.....	۷۶
چگونه پوشه محافظت شده را به حالت عادی برگردانیم؟.....	۷۸
فصل سوم : مخفی کردن اطلاعات با نرم‌افزار ساده Plain Sight.....	۸۱
معرفی و آشنایی با نرم‌افزار.....	۸۱

۸۳	مخفی سازی اطلاعات در قالب یک فایل دیگر
۸۷	بازیابی فایل مخفی شده
۹۱	فصل چهارم : رمزنگاری متن ها با نرم افزار ساده BC Text Encoder
۹۱	آشنایی با نرم افزار
۹۲	رمزنگاری یک متن
۹۴	رمزگشایی یک متن رمزنگاری شده

پیشگفتار

یکی از مهم‌ترین و جالب‌ترین مسائلی که در دنیای کامپیوترهای شخصی مطرح است، بحث حفاظت از اطلاعات و جلوگیری از دسترسی افراد متفرقه به برخی اطلاعات خاص می‌باشد. قطعاً همه ما اطلاعاتی داریم که تصور لو رفتن این اطلاعات، خواب را از چشمانمان می‌گیرد. اطلاعاتی چون اسناد مهم اداری، اسناد مالی، تصاویر و فیلم‌های خانوادگی، فرمولاسیون‌ها، برنامه‌های ساخته شده توسط خودمان و ...

حالا این سوال را از شما می‌پرسیم که آیا شما برای حفاظت از اسناد و اطلاعات مهم داخل کامپیوترتان کاری کرده‌اید؟

در این زمینه اگر پاسخ شما منفی است، هر چه زودتر دست به کار شوید تا بعداً برایتان پشیمانی به وجود نیاید که آن زمان پشیمانی سودی نخواهد داشت.

برنامه‌های زیادی در این زمینه وجود دارند که ما از طریق آنها می‌توانیم به مخفی کردن، قفل‌گذاری روی اطلاعات، رمزنگاری متن‌ها و ... پردازیم. هر نرم‌افزاری خوبی و بدی‌هایی را دارد. ما قبل از نگارش کتاب، اکثر نرم‌افزارهای کاربردی این حوزه را تست کرده‌ایم و سعی کردیم با انتخاب بهترین نرم‌افزارها، بهترین بازدهی را برای شما فراهم کنیم.

این کتاب برای چه کسانی است؟

همان‌طور که گفته شد، همه‌ی ما اسناد زیادی داریم که نباید در دسترس همگان باشد. بنابراین کسانی که می‌خواهند اطلاعات سری خود را از دسترس دیگران مخفی کنند، کسانی که می‌خواهند گاو صندوقی در کامپیوتر

خود ایجاد و اطلاعات با اهمیت خود را در آن قرار دهند، کسانی که می‌خواهند روی برخی پوشه‌های کامپیوتر خود قفل گذاری کنند، کسانی که می‌خواهند متن ارسالی به دیگران را رمزنگاری نموده و سپس برای طرف مقابل بفرستند، کسانی که می‌خواهند کامپیوتر خود را به مرکز تعمیرات ببرند یا آن را به فروش برسانند، برای حفظ امنیت اطلاعاتشان می‌توانند از این کتاب استفاده کنند.

انتشارات کلید آموزش با ایجاد پایگاه اینترنتی به نام انجمن گفتگوی کلید، از سوالات و انتقادات شما در زمینه کتابهای کلید استقبال می‌کند. بنابراین شما خوانندگان گرامی برای بیان سوالات و بیانات خود می‌توانید به آدرس اینترنتی <http://kelid.ir/forum> مراجعه کرده و پس از ثبت نام در این انجمن، دیدگاه‌های خود را مطرح نمایید.

فصل اول

نرم افزار Steganos Privacy Suit

تاکنون تصور کرده‌اید که اگر مثلاً عکس‌های خانوادگی شما روی اینترنت پخش شود چه حالی خواهید داشت؟ تاکنون به این فکر کرده‌اید که این همه فیلم‌های خانوادگی چطور بین مردم دست به دست می‌شود و خیلی‌ها در نتیجه‌ی آن درگیر مشکلات بسیار جدی می‌شوند؟ تاکنون توجه کرده‌اید که اگر فایل‌های خصوصیتان به دست افراد ناباب بیفتد چه خطراتی شما را تهدید می‌کند؟

اگر بخواهید کامپیوترتان را برای تعمیر به مرکز خدماتی ناشناخته ببرید چه می‌کنید؟ آیا همه اطلاعات را از روی هارد دیسک پاک می‌کنید؟ برای اینکه همه‌ی این نگرانی‌ها و ابهامات را از ذهن خود برطرف کنید، با ما همراه شوید ...

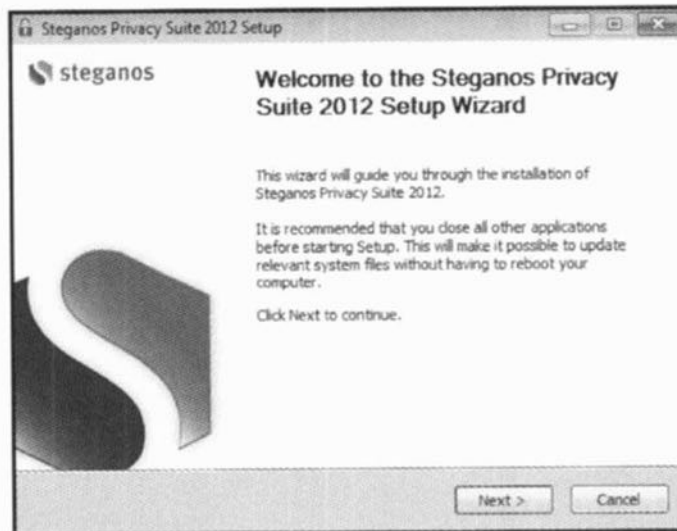
شرکت‌های تولید کننده‌ی نرم‌افزار توانسته‌اند با تولید نرم‌افزارهای امنیتی، بخشی از نگرانی‌هایی که در بالا به آن‌ها ذکر شد را برطرف کنند. Steganos یکی از شرکت‌های نرم‌افزارهای امنیتی است که محصولات متفاوت و قدرتمندی را در زمینه‌های مختلف امنیتی و به اصطلاح Security&Privacy عرضه نموده است.

بسته‌ی امنیتی مشهور و قدرتمند این شرکت تحت عنوان Steganos Security Suite مجموعه‌ای کامل از ابزارهای گوناگون امنیتی در زمینه‌های امنیت اطلاعات، امنیت در مقابل نرم‌افزارهای مخرب، امنیت فعالیت‌ها و ... است.

نرم افزار Steganos Security Suit شامل اکثر راه های ممکن برای رمز گذاری و مخفی کردن اطلاعات است. این نرم افزار امکاناتی چون پشتیبانی کامل از فایل های آفیس، قفل کردن اطلاعات، پاک کردن فایل بدون کوچکترین شانس بازیابی، کار با دیسک های رمزنگاری شده مجازی، تمیز کردن تاریخچه، پشتیبانی از انواع ایمیل و نرم افزارهای مربوطه، موتورهای جستجو، کوکی ها، cache و ... را به ارمغان می آورد.

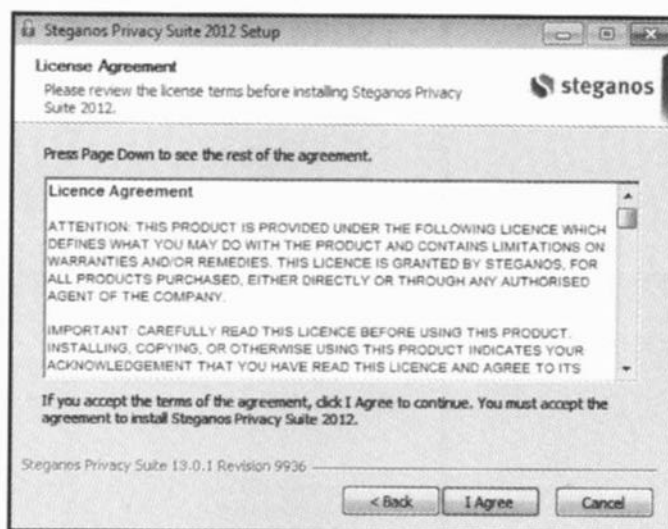
درس اول: نصب و آشنایی با محیط نرم افزار Steganos Security Suit

ابتدا روی فایل Steganos Privacy Suit.exe جفت کلیک می کنیم. اولین پنجره از عملیات نصب نمایش داده می شود. در این پنجره روی دکمه Next کلیک می کنیم (تصویر ۱).



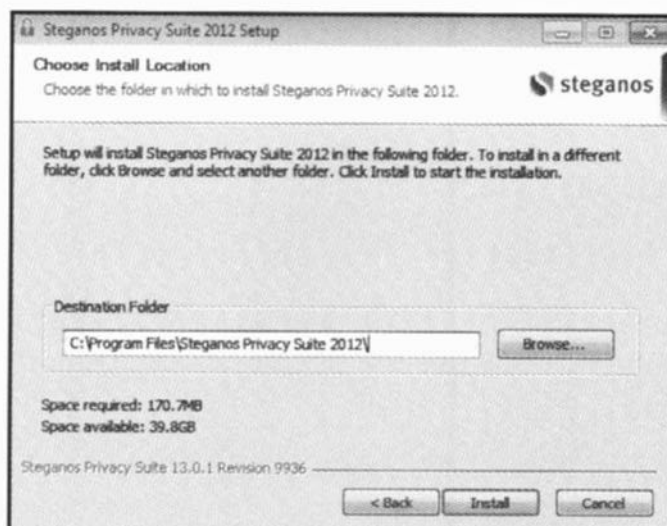
تصویر ۱

در پنجره بعدی نیز روی دکمه Agree کلیک می کنیم تا به پنجره بعدی برویم (تصویر ۲).



تصویر ۲

در این پنجره مسیر نصب نرم افزار را می توانیم تعیین کنیم. ما این قسمت را بدون تغییر گذاشته و روی **Install** کلیک می کنیم و صبر می کنیم تا عملیات نصب به پایان برسد (تصویر ۳).



تصویر ۳

بعد از پایان نصب، پنجره ای مانند تصویر ۴ ظاهر می شود. در این پنجره روی **Finish** کلیک کرده و منتظر می مانیم تا سیستم ریست شود تا عملیات نصب به درستی انجام پذیرد.

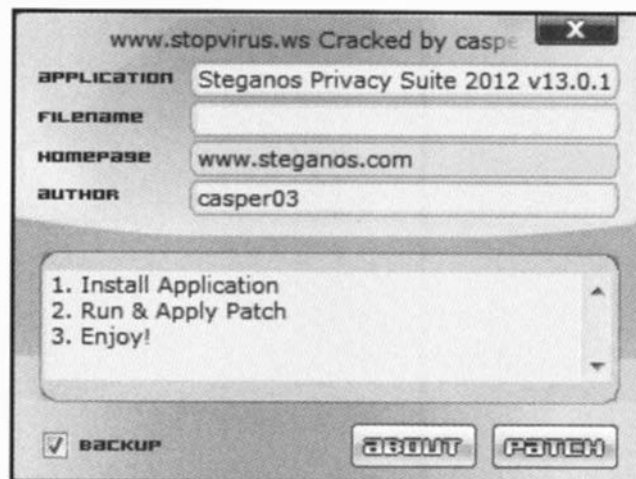


تصویر ۴

اکنون این نرم‌افزار در رایانه نصب شده است ولی موقتی یعنی ۳۰ روزه می‌باشد و پس از آن به طور خودکار غیر فعال می‌شود. برای حل این مشکل و دائمی کردن برنامه، وارد پوشه Crack این نرم‌افزار که در کنار فایل نصبی آن موجود است می‌شویم.

در این پوشه فایل‌ای به نام Patch.exe قرار دارد. این فایل را در همان جایی که نرم‌افزار را نصب کرده‌ایم یعنی مثلاً مسیر C:\Program Files\Steganos Privacy Suite 2012 کپی می‌کنیم.

اگر از ویندوز 7 یا Vista استفاده می‌کنیم برای اجرای این فایل روی آن راست کلیک کرده و سپس گزینه Run as administrator را انتخاب می‌کنیم. ولی اگر ویندوز ما XP باشد می‌توانیم مستقیماً روی آن جفت کلیک کنیم. با اجرای فایل، پنجره‌ای مانند تصویر ۵ ظاهر می‌شود.



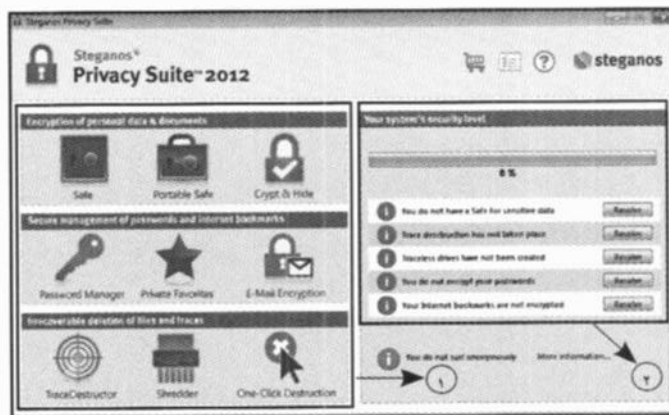
تصویر ۵

روی دکمه‌ی Patch کلیک می‌کنیم و صبر می‌کنیم تا پیغام PATCHING DONE نمایش داده شود (تصویر ۶).



تصویر ۶

حالا این نرم‌افزار از حالت موقتی به حالت دائمی تبدیل شده است. این پنجره را می‌بندیم. نرم‌افزار Steganos Privacy Suit را از روی دسکتاپ اجرا می‌کنیم تا وارد محیط آن شویم. (تصویر ۷)



تصویر ۷

محیط کاربری این نرم‌افزار بسیار ساده و در عین حال جذاب طراحی شده است. همان طور که در تصویر ۷ مشاهده می‌کنیم این محیط از دو قسمت تشکیل شده است.

در قسمت ۱ ابزارهای این نرم‌افزار قرار دارد که هر کدام از آنها ویژگی‌های کاربردی و جالبی را در خود جای داده‌اند.

در قسمت ۲ وضعیت امنیتی رایانه چک می‌شود. نرم‌افزار Steganos Privacy Suit در هر لحظه بررسی می‌کند که آیا از امکانات امنیتی این نرم‌افزار استفاده شده است یا خیر؛ و بر اساس آن درصد امنیت سیستم را برآورد می‌کند. در این لحظه ما از هیچ یک از این امکانات استفاده نکرده‌ایم پس در نتیجه میزان درصد نمایش داده شده در قسمت ۲ روی عدد صفر می‌باشد. در ادامه با امکانات امنیتی و کاربردی این نرم‌افزار آشنا خواهیم شد.

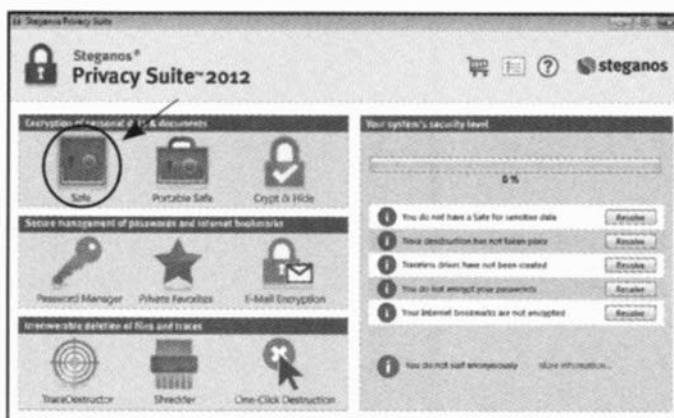
درس دوم: ایجاد یک گاو صندوق الکترونیکی (فضای امن) برای ذخیره اطلاعات

در این درس می‌خواهیم یک فضای مجازی برای قرار دادن اطلاعات محرمانه ایجاد کنیم. در واقع می‌خواهیم نوعی گاو صندوق داشته باشیم که جز خودمان هیچ کس دیگری نتواند به فایل‌های درون آن دسترسی داشته

باشد. نرم افزار Steganos Privacy Suit این قابلیت را در ابزاری به نام Safe قرار داده است.

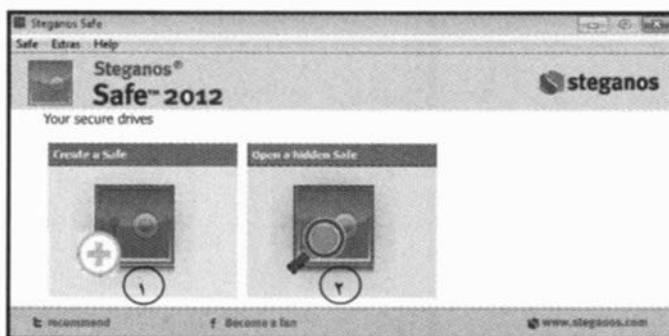
ابزار Safe یک گاوصندوق بزرگ و قوی برای حفاظت از اطلاعات محرمانه ما ایجاد می کند. این ابزار از جدیدترین سیستم امنیتی به نام AES یا همان Advanced Encryption Standard استفاده می کند و به ما این توانایی را می دهد که تا ۲۵۶ گیگابایت اطلاعات از هر نوع فرمتی را در این گاوصندوق جای دهیم.

برای ایجاد یک گاوصندوق از پنجره اصلی نرم افزار روی آیکن گاوصندوق که Safe نام دارد کلیک می کنیم (تصویر ۸).



تصویر ۸

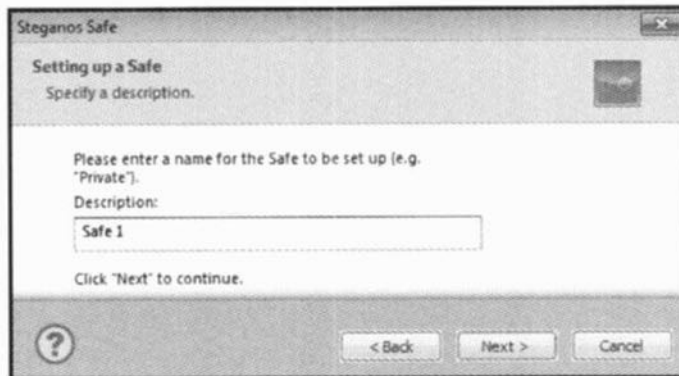
با کلیک روی این آیکن، پنجره Steganos Safe باز می شود که شامل دو گزینه می باشد (تصویر ۹).



تصویر ۹

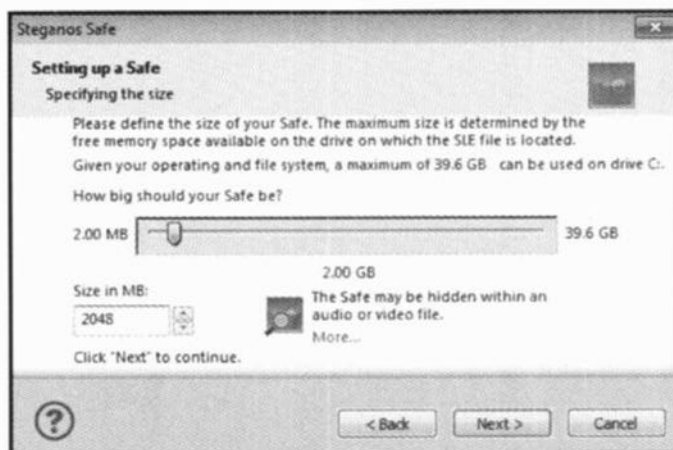
در کادر شماره ۱ از تصویر ۹ که **Create a Safe** نام دارد می توانیم گاو صندوق جدیدی ایجاد کنیم.

در کادر شماره ۲ که **Open a hidden Safe** نام دارد می توانیم گاو صندوق مخفی شده ای که قبلا ساخته ایم را باز کنیم (بعدا به آن اشاره خواهیم کرد). برای ایجاد یک گاو صندوق روی کادر شماره ۱ از پنجره ی تصویر ۹، کلیک می کنیم تا پنجره مربوط به آن ظاهر شود. در پنجره ی ظاهر شده روی دکمه **Next** کلیک می کنیم تا وارد مرحله بعد شویم (تصویر ۱۰).



تصویر ۱۰

در این پنجره می توانیم نامی را برای گاو صندوق انتخاب کنیم. ما نام این گاو صندوق را **Safe1** می گذاریم و سپس روی دکمه **Next** کلیک می کنیم تا پنجره بعدی باز شود (تصویر ۱۱).



تصویر ۱۱


در این پنجره باید حجم گاو صندوقمان را تعیین کنیم. ما به اندازه فضای خالی درایوی که ویندوز در آن نصب شده است و حداکثر تا ۲۵۶ گیگابایت می‌توانیم فضا یا حجم به این گاو صندوق اختصاص دهیم. به عنوان مثال درایو C رایانه ما که ویندوز در آن قرار دارد، ۶/۳۹ گیگابایت فضای خالی دارد. در نتیجه حداکثر حجمی که به گاو صندوقمان می‌توانیم اختصاص دهیم ۶/۳۹ گیگابایت می‌باشد.

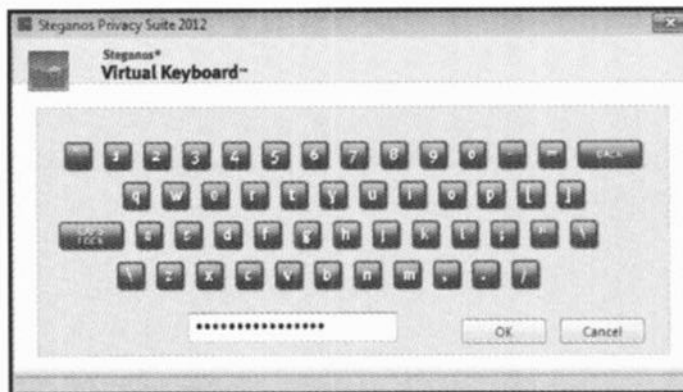
ما میزان حجم این گاو صندوق را روی ۲ گیگابایت تنظیم می‌کنیم تا بتوانیم به همین میزان، اطلاعات در داخل آن قرار دهیم. سپس روی دکمه **Next** کلیک می‌کنیم تا پنجره مربوط به تعیین پسورد ظاهر شود (تصویر ۱۲).



تصویر ۱۲

یکی از امکانات امنیتی این نرم‌افزار، ارائه روشی برای جلوگیری از جاسوسی نرم‌افزارهای کی لاگر (Key Logger) می‌باشد. این نرم‌افزارها معمولاً توسط افرادی که از رایانه ما به اشتراک استفاده می‌کنند و یا هکرها یا جاسوسان اینترنتی، در رایانه نصب می‌شوند و لیستی از همه کلیدهای فشرده شده در کامپیوتر را برای هکر مورد نظر ارسال می‌کنند.

نرم‌افزار Steganos Privacy Suit برای جلوگیری از جاسوسی این برنامه‌ها یک صفحه کلید مجازی برای وارد کردن پسورد در اختیار ما قرار داده است. استفاده از صفحه کلید مجازی سبب می‌شود که نرم‌افزارهای جاسوسی و Key Logger ها نتوانند پسوردهای وارد شده توسط ما را ثبت و ذخیره کنند. برای استفاده از این صفحه کلید می‌توانیم روی آیکن  در پنجره تصویر ۱۲ کلیک کنیم و با استفاده از صفحه کلید گرافیکی که نمایش داده می‌شود پسورد موردنظرمان را وارد کنیم (تصویر ۱۳).

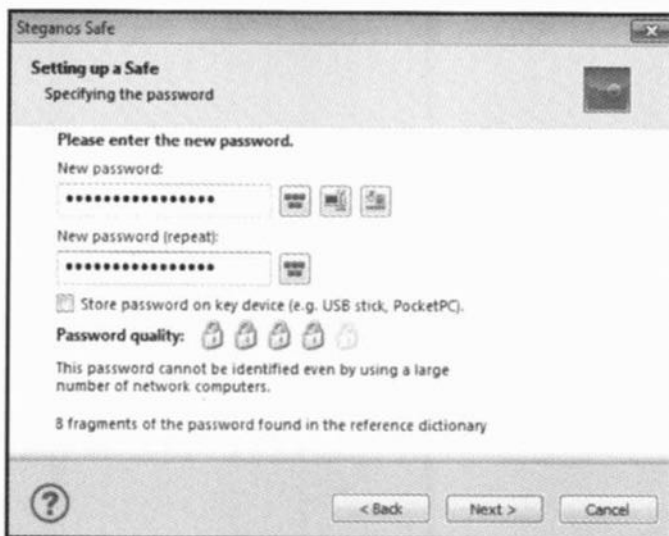


تصویر ۱۳

نکته ...

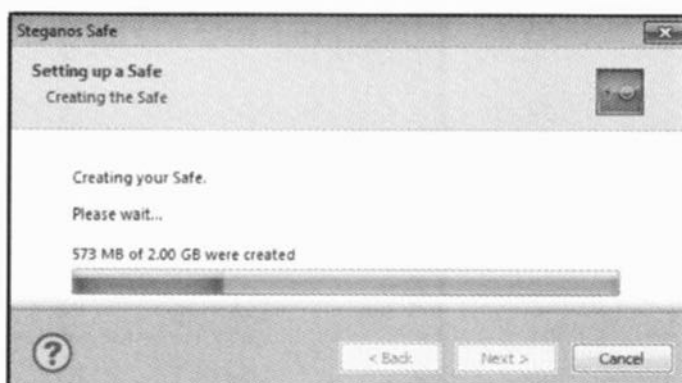
پسوردها را باید به گونه‌ای انتخاب کنیم که قابل حدس زدن توسط دیگران نباشد و فقط خودمان آن را به خاطر داشته باشیم تا امنیت اطلاعاتمان به خطر نیفتد. بهتر است پسوردی انتخاب کنیم که ترکیبی از اعداد و حروف و علائم باشد تا احتمال حدس زدن آن بسیار کاهش یابد و تقریباً غیر ممکن شود.

در پنجره مربوط به تعیین پسورد، پسورد موردنظرمان را در کادر New password وارد می‌کنیم. در کادر New password (repeat) نیز همان پسورد را دوباره وارد می‌کنیم تا نرم‌افزار اطمینان حاصل کند که عبارت وارد شده اشتباه نمی‌باشد (تصویر ۱۴).



تصویر ۱۴

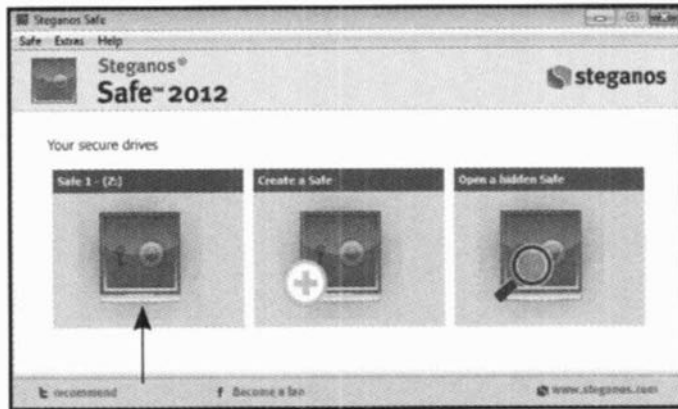
در قسمت Password quality میزان امنیت پسورد وارد شده از ۱ تا ۵ درجه بندی می‌شود. همان طوری که در تصویر ۱۴ مشاهده می‌کنیم ۴ عدد از تصاویر قفل‌ها روشن شده است یعنی امنیت پسورد انتخابی ما درجه ۴ است که قابل قبول می‌باشد. حالا روی دکمه Next کلیک می‌کنیم و صبر می‌کنیم تا گاو صندوق ایجاد شود (تصویر ۱۵).



تصویر ۱۵

سپس در پنجره بعدی روی دکمه Finish کلیک می‌کنیم.

اکنون مشاهده می‌کنیم که در پنجره Steganos Safe گاوصندوق جدیدی با نام (Z:) - Safe 1 تولید شده است (تصویر ۱۶).



تصویر ۱۶

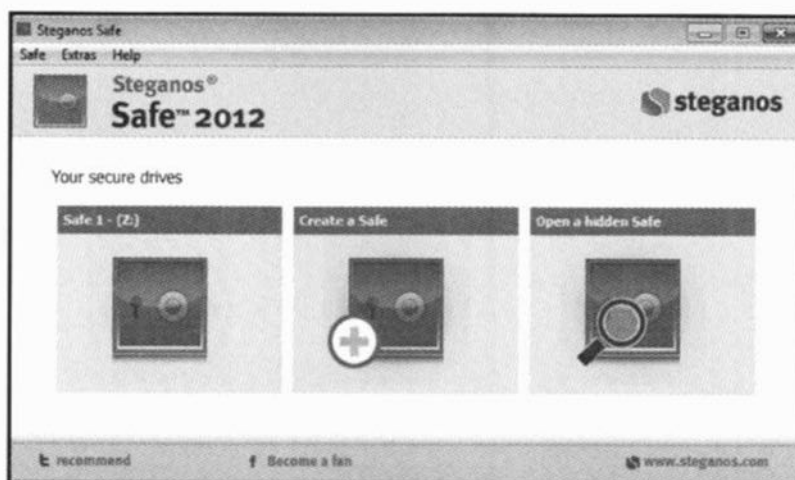
Safe 1 همان نامی است که خودمان برای گاوصندوق انتخاب کرده‌ایم. (Z:) در واقع نام یک درایو مجازی است که خود نرم‌افزار به آن اختصاص داده است همانند سایر درایوهای رایانه نظیر درایو C یا D و... با این تفاوت که درایو Z یک درایو مجازی می‌باشد و در واقع خودش در درایو C قرار دارد.

درس سوم: ورود به گاوصندوق و تنظیمات مربوط به آن

در بخش قبل آموختیم که چطور یک گاوصندوق برای قرار دادن اطلاعات ایجاد کنیم. در این بخش می‌خواهیم روش باز کردن و بستن (ورود و خروج) گاوصندوق و هم چنین تنظیمات مربوط به آن را توضیح دهیم.

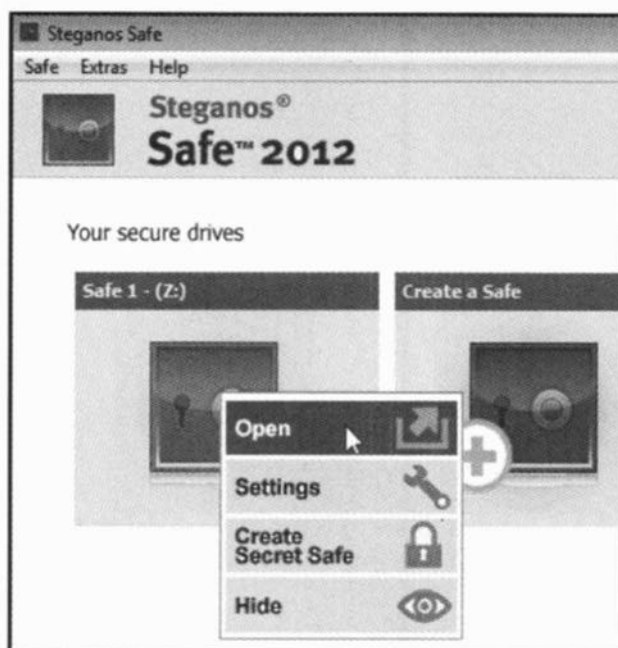
بازکردن و ورود به گاوصندوق:

برای باز کردن و ورود به گاوصندوق مراحل زیر را دنبال می‌کنیم: ابتدا نرم‌افزار Steganos Privacy Suit را اجرا می‌کنیم و سپس به قسمت Safe وارد می‌شویم (تصویر ۱۷).



تصویر ۱۷

حال روی گاو صندوق 1 Safe راست کلیک کرده و از منوی باز شده گزینه Open را انتخاب می‌کنیم (تصویر ۱۸).




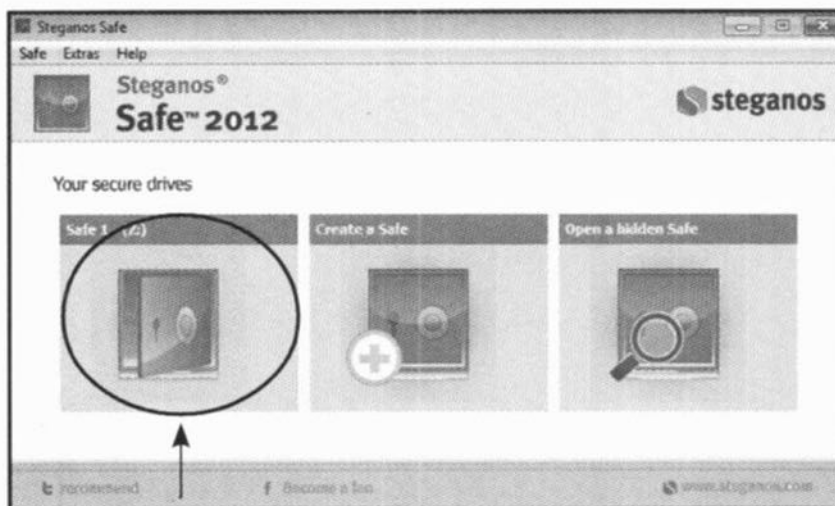
تصویر ۱۸

در پنجره باز شده پسوردی که برای این گاو صندوق انتخاب کرده بودیم را وارد می‌کنیم (تصویر ۱۹).



تصویر ۱۹

اگر پسوردی که قبلا انتخاب کردیم از نوع تصویری بود باید با کلیک روی آیکن  تصاویر موردنظر را به ترتیب انتخاب می‌کردیم. در ادامه روش تعیین پسورد تصویری آموزش داده خواهد شد. حالا روی دکمه OK کلیک می‌کنیم. در این حالت مشاهده می‌کنیم که تصویر گاوصندوق با در بسته به یک گاوصندوق با در باز تبدیل شده است (تصویر ۲۰).



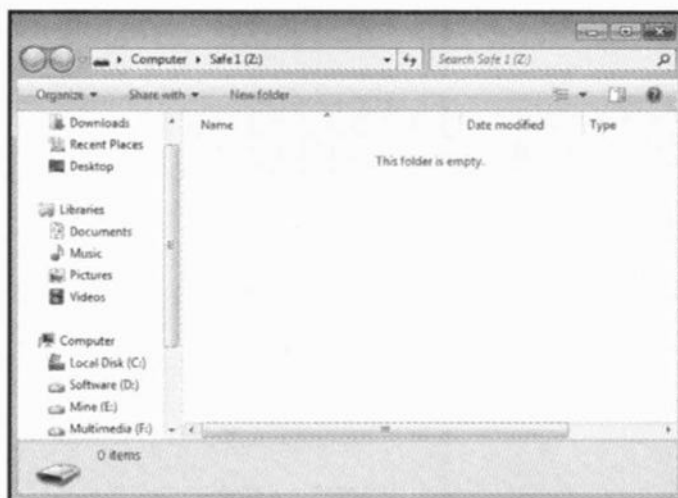
تصویر ۲۰

حال روی این گاوصندوق راست کلیک کرده و گزینه Display را انتخاب می‌کنیم (تصویر ۲۱).



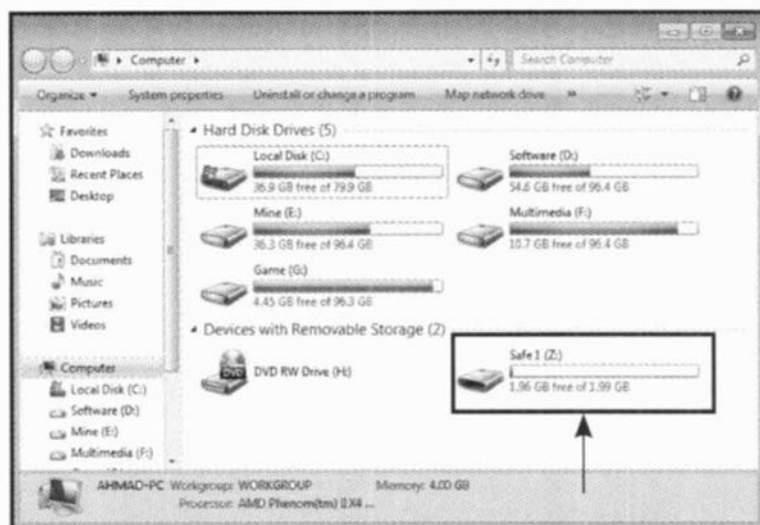
تصویر ۲۱

با انتخاب این گزینه درایو مجازی Z که همان پنجره گاو صندوق Safe1 می باشد در یک پنجره باز می شود (تصویر ۲۲).



تصویر ۲۲

البته وقتی پسورد را برای باز کردن گاو صندوق وارد کردیم درایو مجازی مربوط به آن یعنی Z در My Computer ویندوز ظاهر می شود و از آن جا نیز می توانیم وارد این گاو صندوق شویم (تصویر ۲۳).

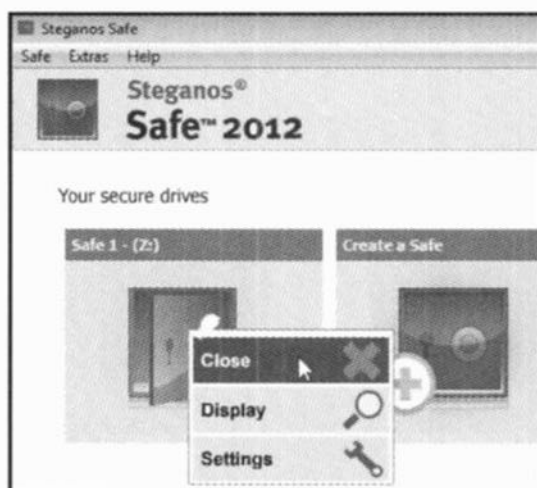


تصویر ۲۳

انتقال فایل‌ها به گاو صندوق مانند سایر درایوها انجام می‌شود. یعنی تا وقتی که گاو صندوق ما باز است می‌توانیم هر نوع فایل با هر فرمتی را در گاو صندوق کپی کنیم. هم چنین هیچ محدودیتی برای اجرای فایل‌ها وجود ندارد و گاو صندوق ما عملکردی مشابه با بقیه درایوهای سیستم دارد.

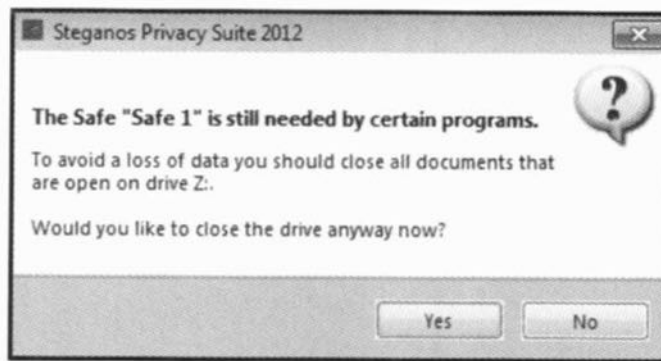
بستن گاو صندوق :

برای بستن گاو صندوق کافی است روی آیکن گاو صندوق Safe1 در پنجره Steganos Safe راست کلیک کنیم و از منوی باز شده، گزینه Close را انتخاب کنیم (تصویر ۲۴).



تصویر ۲۴

با این کار پنجره جدیدی باز می‌شود که برای بستن فایل‌های موجود در این گاو صندوق به شما هشدار می‌دهد. با کلیک روی دکمه Yes گاو صندوق دوباره به حالت بسته در می‌آید (تصویر ۲۵).



تصویر ۲۵

با بستن گاو صندوق، درایو مجازی مربوط به آن از My Computer حذف می‌شود و تا زمانی که دوباره گاو صندوق را باز نکنیم قابل دسترسی نخواهد بود.

تنظیمات مربوط به گاو صندوق :

برای وارد شدن به بخش تنظیمات ویندوز بهتر است ابتدا گاو صندوق را ببندیم. سپس با راست کلیک روی آیکون گاو صندوق Safe 1 گزینه Settings را انتخاب کنیم (تصویر ۲۶).



تصویر ۲۶

با این کار پنجره‌ای ظاهر می‌شود

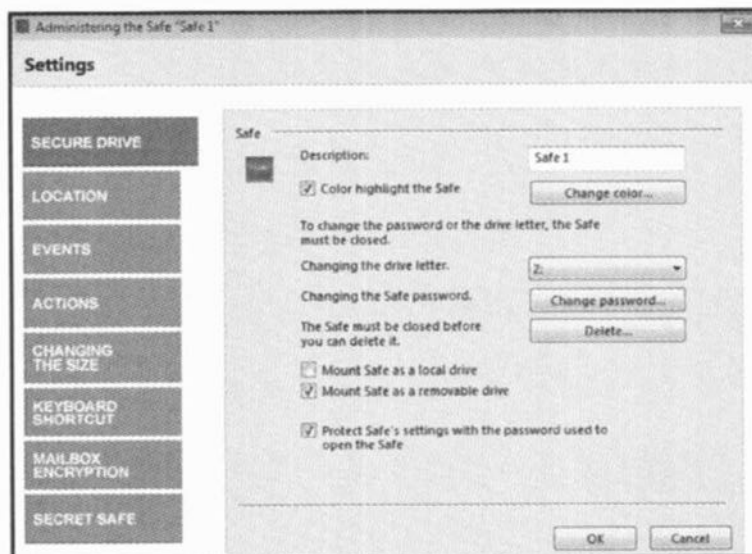
که پسورد گاو صندوق Safe 1 را در آن وارد می‌کنیم (تصویر ۲۷).



تصویر ۲۷

با کلیک روی دکمه OK وارد پنجره تنظیمات این گاوصندوق می شویم (تصویر ۲۸).

در سمت چپ تعدادی سربرگ آبی رنگ دیده می شود که با کلیک روی هر کدام از آنها گزینه های متفاوتی را در صفحه اصلی خواهیم دید. در ادامه گزینه های مهم این سربرگ ها را بررسی می کنیم.



تصویر ۲۸

سربرگ **SECURE DRIVE** :

در قسمت Description می توانیم نام گاوصندوق را تغییر دهیم. با فعال کردن گزینه Color highlight the Safe می توانیم رنگ آیکن گاوصندوق را در نرم افزار تغییر دهیم.

در قسمت **Changing the drive letter** می‌توانیم نام درایو مجازی مربوط به این گاوصندوق را تغییر دهیم.

با کلیک روی دکمه **Change password** می‌توانیم پسورد این گاوصندوق را تغییر دهیم. به این ترتیب که ابتدا پسورد فعلی را وارد کرده و در مرحله بعد پسورد جدید را وارد می‌کنیم.

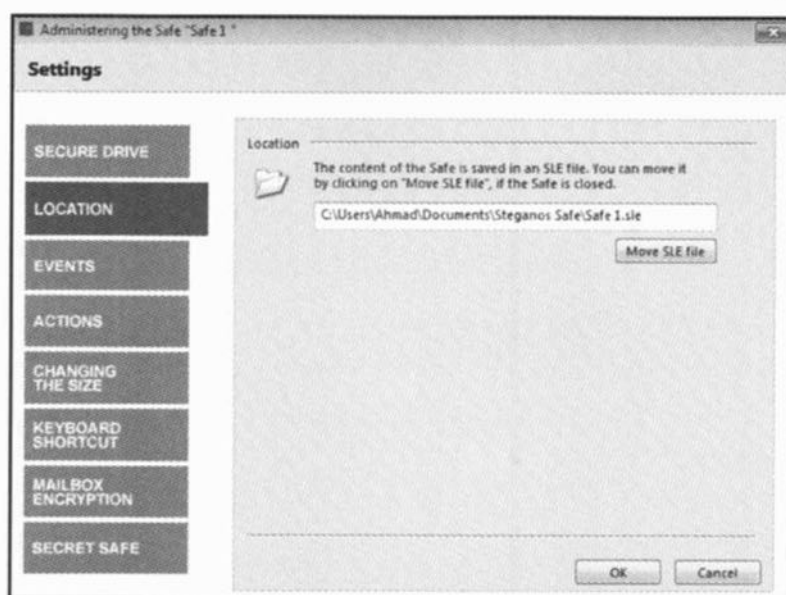
با کلیک روی دکمه **Delete** می‌توانیم گاوصندوق را حذف کنیم. با این کار گاوصندوق به همراه تمامی محتویات آن از بین می‌رود پس قبل از انجام این کار از تصمیم خود مطمئن باشید.

فعال کردن گزینه **Protect Safe's settings with the password...**

باعث می‌شود کاربر مجبور شود برای ورود به تنظیمات گاوصندوق، پسورد آن را وارد کند.

سربرگ LOCATION :

در این سربرگ می‌توانیم مکان قرارگرفتن گاوصندوق در هارد دیسک را تغییر دهیم (تصویر ۲۹).

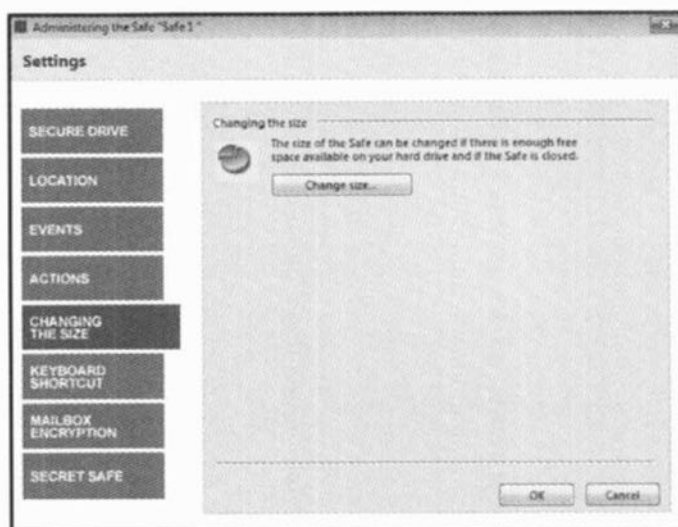


تصویر ۲۹

مثلاً اگر می‌خواهیم حجم گاو صندوق را بیشتر کنیم می‌توانیم آن را به درایوی منتقل کنیم که فضای خالی بیشتری دارد. در کل بهتر است گاو صندوقمان را در درایوی غیر از درایو C که درایو ویندوزمان می‌باشد ذخیره کنیم تا با تعویض ویندوز، گاو صندوق و اطلاعات داخل آن از بین نرود.

سربزرگ CHANGING THE SIZE

در این سربزرگ از پنجره تنظیمات با کلیک روی دکمه Change size پنجره جدیدی باز می‌شود که پسورد گاو صندوق را از ما می‌خواهد. پس از وارد کردن پسورد می‌توانیم حجم گاو صندوق را به مقدار دلخواه تغییر دهیم (تصویر ۳۰).




تصویر ۳۰

درس چهارم: ایجاد پسوردی قوی و مطمئن

یکی از ویژگی‌های مهم نرم‌افزار Steganos Privacy Suit که آن را از سایر نرم‌افزارهای موجود، متمایز می‌کند ارائه ۲ روش برای تولید پسوردی مطمئن می‌باشد که در ادامه به توضیح آن‌ها می‌پردازیم:

روش اول :

در این روش انتخاب پسوردی مطمئن را به نرم افزار محول می کنیم. برای این کار در پنجره تعیین پسورد روی آیکن  که Generate password نام دارد کلیک می کنیم (تصویر ۳۱).



تصویر ۳۱

پنجره جدیدی با نام Generate password ظاهر می شود (تصویر ۳۲).



تصویر ۳۲

در این پنجره با اعمال یک سری شرایط می‌توانیم پسورد دلخواه و در عین حال مطمئنی را تولید کنیم.

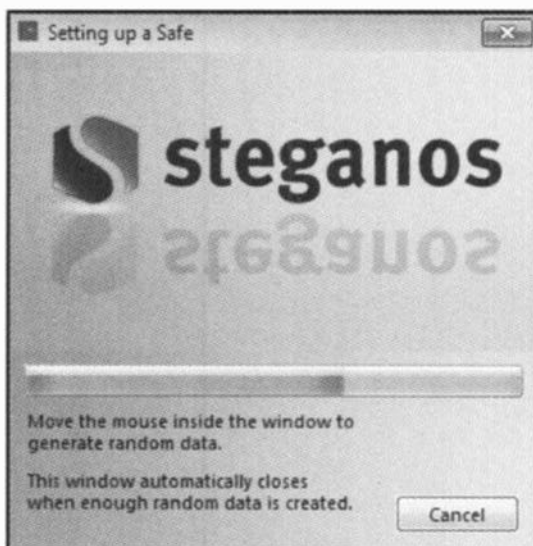
در قسمت Number of characters می‌توانیم تعداد کاراکتر پسورد را تعیین کنیم. ما این گزینه را روی عدد ۱۲ قرار می‌دهیم.

فعال بودن گزینه Use lowercase نرم‌افزار را مجاب می‌کند که از حروف کوچک نیز در پسورد استفاده کند.

فعال بودن گزینه Use UPPERCASE نرم‌افزار را مجاب می‌کند که از حروف بزرگ نیز در پسورد استفاده کند.

فعال بودن گزینه Use numbers نرم‌افزار را مجاب می‌کند که از اعداد نیز در پسورد استفاده کند.

فعال بودن گزینه Use special characters نرم‌افزار را مجاب می‌کند که از علامت‌های خاص دیگری نظیر @، ^، *، |، & و... نیز در پسورد استفاده کند.



تصویر ۳۳

ما همه این گزینه‌ها را فعال می‌کنیم تا امنیت پسورد بالاتر رود.

حالا روی دکمه Next کلیک می‌کنیم تا پنجره بعدی نمایش داده شود (تصویر ۳۳).

این ابزار طوری طراحی شده است که با حرکت نشانگر ماوس در این پنجره کاراکترهای تصادفی را برای پسورد در نظر می‌گیرد. یعنی باید

نشانگر ماوس را آن قدر در پنجره تصویر ۳۳ حرکت دهیم تا عملیات انتخاب پسورد به پایان برسد.

بعد از اتمام این مرحله، پنجره جدیدی باز می شود که پسورد تولید شده در آن به صورت نقطه های سیاه رنگ نمایش داده می شود (تصویر ۳۴).



تصویر ۳۴

در این پنجره با کلیک روی دکمه در پوشه می توانیم کاراکترهای پسورد تولید شده را مشاهده کنیم (تصویر ۳۵).

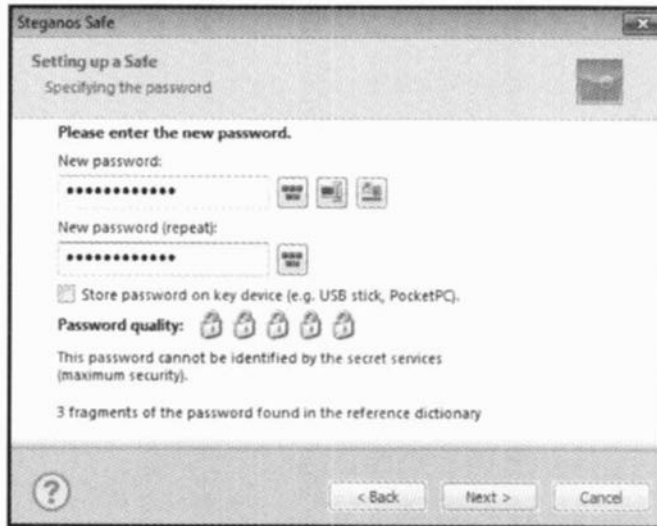


تصویر ۳۵

برای اطمینان بهتر است پسورد تولید شده را در جایی امن یادداشت کنیم و یا با استفاده از ابزار مدیریت پسورد که در ادامه به توضیح آن می پردازیم، از آن نگهداری کنیم.

حال روی OK کلیک می کنیم تا پسورد تایید شود با این کار به پنجره مربوط به تعیین پسورد باز می گردیم. با توجه به قسمت

Password quality مشاهده می‌کنیم که این پسورد از درجه امنیتی بالایی نیز برخوردار است (تصویر ۳۶).




تصویر ۳۶

روش دوم :

این نرم‌افزار روش دیگری نیز برای تعیین پسورد در اختیار ما قرار داده است. در این روش با استفاده از تصاویر و ترتیب انتخاب آن‌ها می‌توانیم پسورد امنی را تولید کنیم.



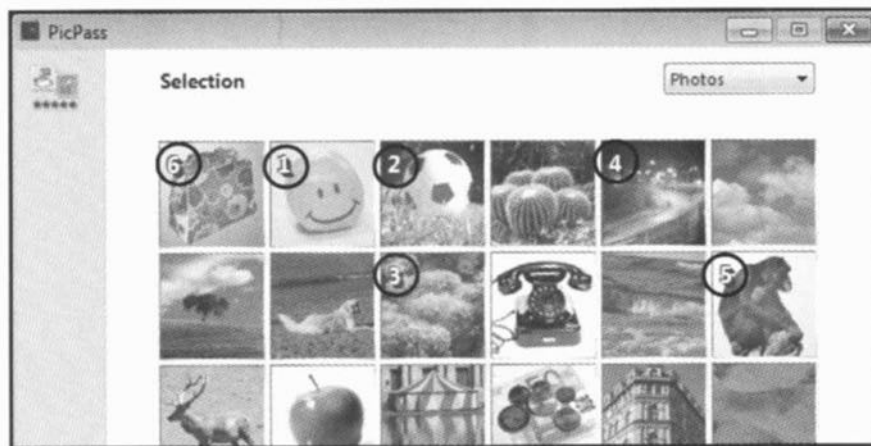
تصویر ۳۷

برای این کار در پنجره‌ی تصویر شماره ۳۶ بر روی آیکن  که Select password using PicPass نام دارد کلیک می‌کنیم تا پنجره PicPass باز شود (تصویر ۳۷).

در این پنجره با کلیک روی یک تصویر، شماره ۱ به آن اختصاص داده می‌شود. با کلیک روی تصویر بعدی، شماره ۲ به آن تصویر اختصاص داده می‌شود. این کار را حداکثر تا ۳۶ بار می‌توانیم ادامه دهیم چون تعداد تصاویر موجود در این پنجره ۳۶ عدد می‌باشد.

بعد از این که تصاویری را به ترتیب دلخواه انتخاب کردیم روی دکمه Repeat کلیک می‌کنیم تا به همان ترتیب انتخاب را دوباره تکرار کنیم. این کار به خاطر این است که نرم‌افزار مطمئن شود که تصاویر را همانند مرحله اول و به همان ترتیب انتخاب کرده باشیم.

برای نمونه ما می‌خواهیم یک پسورد با انتخاب شش تصویر تولید کنیم. برای این کار روی تصاویر دلخواه‌مان کلیک کرده و ترتیب انتخاب آن‌ها را به خاطر می‌سپاریم (تصویر ۳۸).



تصویر ۳۸

حال با کلیک روی دکمه Repeat همین تصاویر را به همین ترتیب از ۱ تا ۶ دوباره انتخاب می‌کنیم.

سپس روی دکمه OK کلیک می‌کنیم تا پنجره بعدی ظاهر شود (تصویر ۳۹).



تصویر ۳۹

درس پنجم: مخفی کردن یک گاو صندوق در قالب یک فایل

در این پنجره، پسوردی متناظر با ترتیب انتخاب تصاویر که ترکیبی از اعداد و حروف می باشد ارائه شده است. در واقع اگر این پسورد را انتخاب کنیم برای باز کردن گاوصندوق علاوه بر روش انتخاب تصاویر می توانیم همین پسورد متناظر با آن را نیز وارد کنیم. البته به خاطر سپردن پسورد تصویری کمی مشکل می باشد بنابراین در استفاده از این روش باید دقت کافی داشته باشیم.

یکی از قابلیت های جالب نرم افزار Steganos Privacy Suit قابلیت مخفی کردن گاوصندوق در قالب یک فایل دیگر است. به طوری که هیچ تغییری در آن فایل جز حجم آن ایجاد نمی شود. در واقع افراد غیر مجاز با دیدن آن فایل متوجه نمی شوند که گاوصندوق محرمانه ما در داخل آن پنهان شده است.

البته این قابلیت فقط برای گاوصندوق های با حجم کمتر از ۳ گیگا بایت می باشد. پس با این حساب، گاوصندوق Safe 1 که حجم آن ۲ گیگا بایت می باشد قابلیت مخفی شدن را دارد.

برای مخفی کردن گاوصندوق Safe 1 در قالب یک فایل مراحل زیر را

دنبال می کنیم :

ابتدا نرم‌افزار را اجرا کرده و در پنجره اصلی روی Safe کلیک می‌کنیم. سپس روی آیکن گاو صندوق Safe 1 راست کلیک کرده و از منوی باز شده گزینه Hide را انتخاب می‌کنیم (تصویر ۴۰).



تصویر ۴۰

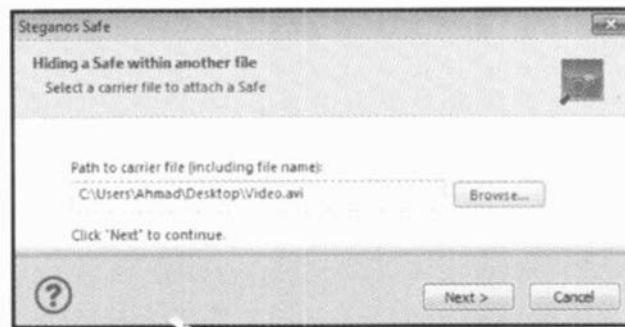
با انتخاب این گزینه پنجره جدیدی باز می‌شود (تصویر ۴۱). در تصویر ۴۱ مشاهده می‌کنیم که فایل‌هایی را که می‌خواهیم گاو صندوق در آن پنهان شود باید یکی از فرمت‌های زیر را داشته باشد:

mp3 , m4a , avi , wmv , exe



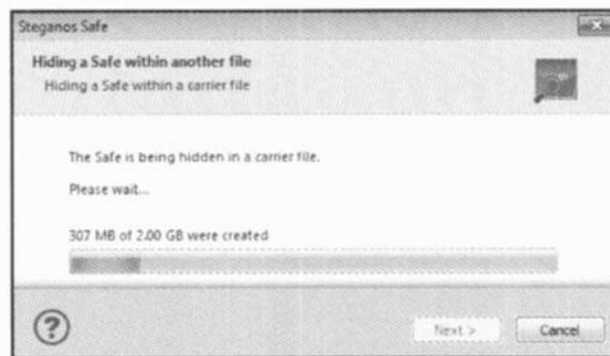
تصویر ۴۱

در این پنجره روی دکمه Next کلیک می‌کنیم تا به مرحله بعد برویم (تصویر ۴۲).



تصویر ۴۲

در این پنجره باید فایلی را که می‌خواهیم گاو صندوق مان در آن مخفی شود را انتخاب کنیم. ما یک فایل ویدئویی با نام Video.avi را انتخاب کرده‌ایم. حال روی دکمه Next کلیک کرده و صبر می‌کنیم تا عملیات مخفی سازی به پایان برسد (تصویر ۴۳).



تصویر ۴۳

پس از این مرحله در پنجره بعدی روی دکمه Finish کلیک می‌کنیم (تصویر ۴۴).



تصویر ۴۴

مشاهده می‌کنیم که با مخفی کردن گاو صندوق Safe 1 در فایل Video.avi این گاو صندوق از پنجره Steganos Safe ناپدید شده است (تصویر ۴۵).



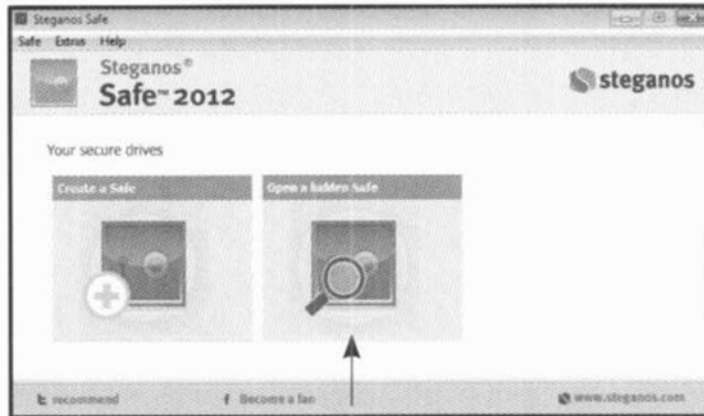
تصویر ۴۵

تا اینجا توانستیم گاو صندوق را در قالب یک فایل ویدئویی پنهان کنیم. یعنی اگر شخصی بخواهد این فایل ویدئویی را اجرا کند، می‌تواند به راحتی این کار را مثل گذشته انجام دهد و هیچ شکمی هم به گاو صندوقی که در پشت آن مخفی شده هست، هم نمی‌کند در واقع افراد غیر مجاز با دیدن این فایل و اجرا کردن آن، متوجه وجود گاو صندوق مخفی ما نخواهند شد. تنها تغییری که در این فایل ویدئویی ایجاد شده است در حجم آن می‌باشد. حجم گاو صندوق Safe 1، دو گیگا بایت است پس در نتیجه به حجم فایل ویدئویی ما، دو گیگا بایت اضافه شده است.

درس ششم: دسترسی به یک گاو صندوق مخفی شده

برای باز کردن و ورود به گاو صندوق مخفی شده در یک فایل مراحل زیر را انجام می‌دهیم:

ابتدا وارد پنجره اصلی نرم افزار می شویم و سپس با کلیک روی Safe وارد پنجره Steganos Safe می شویم. حالا روی آیکن Open a hidden Safe کلیک می کنیم (تصویر ۴۶).



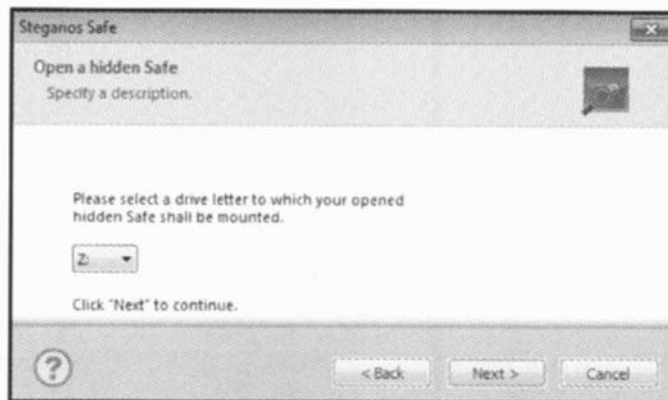
تصویر ۴۶

در پنجره باز شده با کلیک روی دکمه Within which file resides your hidden Safe? همان فایلی که گاو صندوق در آن پنهان شده است را، انتخاب می کنیم (تصویر ۴۷).



تصویر ۴۷

پس از انتخاب آن فایل ویدئویی، پنجره جدیدی باز می شود (تصویر ۴۸).



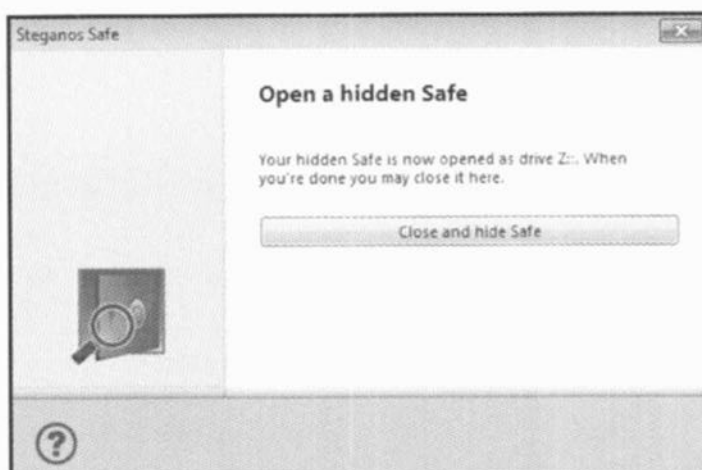
تصویر ۴۸

در این پنجره می‌توانیم نام درایو مجازی مربوط به گاوصندوق را انتخاب کنیم. ما حرف Z را انتخاب می‌کنیم. حالا روی دکمه Next کلیک می‌کنیم. در پنجره بعدی پسورد گاوصندوق Safe 1 را وارد می‌کنیم و بعد از آن روی دکمه Next کلیک می‌کنیم (تصویر ۴۹).



تصویر ۴۹

با این کار گاوصندوق Safe 1 باز شده است و از طریق My Computer می‌توانیم وارد گاوصندوق مان که درایو Z می‌باشد، شویم. هم‌چنین با انجام مراحل فوق، پنجره‌ای نیز باز می‌شود. برای بستن گاوصندوق کافی است روی دکمه Close and hide Safe کلیک کنیم (تصویر ۵۰).



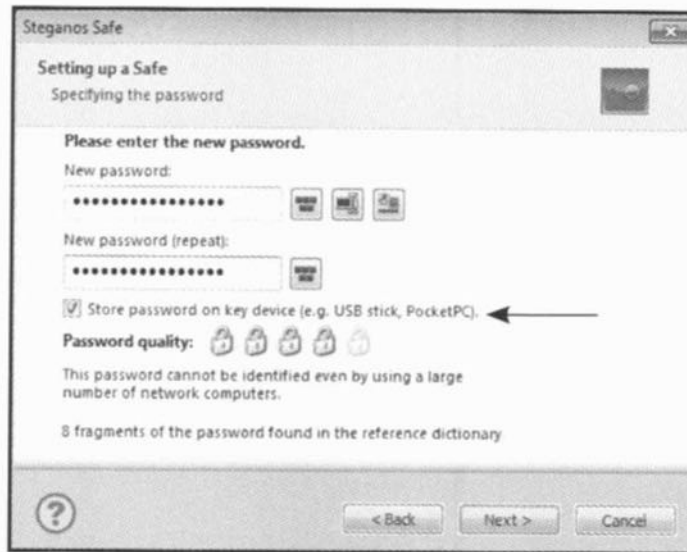
تصویر ۵۰

نکته ...

اگر یک گاوصندوق را در فایل مخفی کنیم دیگر نمی‌توانیم آن گاوصندوق را به حالت عادی برگردانیم. ولی اگر لازم بود که این کار را بکنیم مجبوریم پس از باز کردن گاوصندوق مخفی شده، اطلاعات موجود در آن را در یک گاوصندوق عادی کپی کنیم.

درس هفتم: تبدیل کردن حافظه فلش به کلیدی برای باز کردن گاوصندوق

ما می‌توانیم یک حافظه فلش را به کلیدی برای باز کردن و وارد شدن به گاوصندوق تبدیل کنیم. یعنی با اتصال حافظه فلش به رایانه، برای وارد شدن به گاوصندوق، دیگر نیازی به وارد کردن پسورد نیست. این ویژگی زمانی لازم می‌شود که ما پسورد گاوصندوق را فراموش کرده‌ایم. برای این کار کافی است در هنگام تعیین پسورد علاوه بر دادن پسورد برای گاوصندوق، گزینه `Store password on key device` را نیز فعال کنیم (تصویر ۵۱).



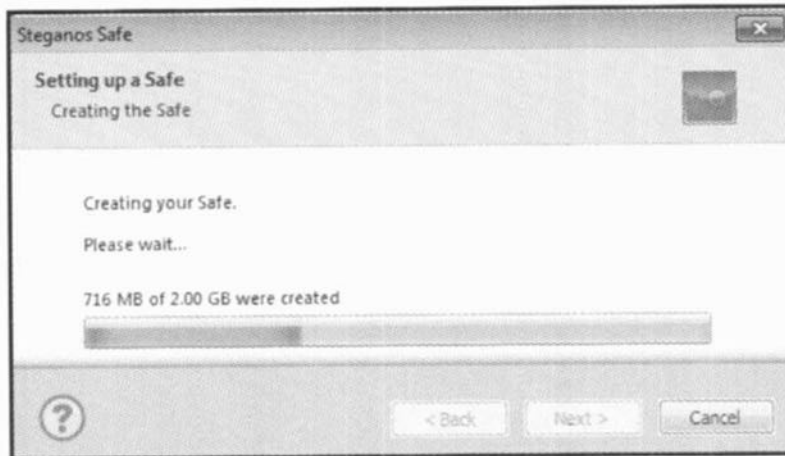
تصویر ۵۱

بعد از فعال کردن این گزینه و وارد کردن پسورد مورد نظرمان باید حافظه فلش را به رایانه متصل کنیم و پس از آن روی دکمه Next کلیک می‌کنیم تا پنجره بعدی باز شود. در پنجره جدید روی نام حافظه فلش کلیک می‌کنیم تا انتخاب شود. سپس روی دکمه OK کلیک می‌کنیم (تصویر ۵۲).



تصویر ۵۲

حال صبر می‌کنیم تا این مرحله به پایان برسد و در پنجره بعدی روی دکمه Finish کلیک می‌کنیم (تصویر ۵۳).



تصویر ۵۳

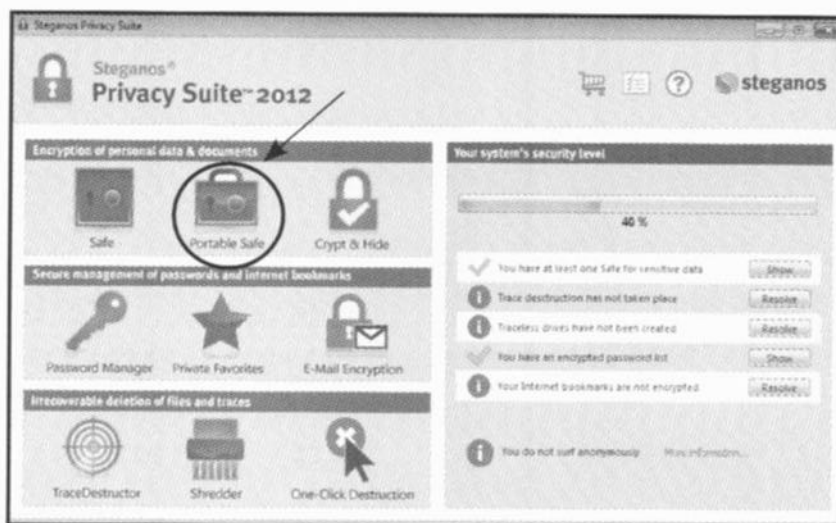
با این کار اگر پسورد را فراموش کردیم، برای باز کردن گاوصندوق کافی است حافظه فلش را به رایانه وصل کنیم. البته اگر این حافظه فلش را فرمت کنیم دیگر نمی‌تواند به عنوان کلید عمل کند.

درس هشتم:

تبدیل حافظه فلش یا لوح فشرده به گاوصندوق

نرم‌افزار Steganos Privacy Suit به ما این امکان را می‌دهد که بتوانیم گاوصندوق را در یک سی دی و یا یک حافظه فلش ایجاد کنیم. ما برای جابه‌جایی اطلاعات مهم خود می‌توانیم از این سیستم امنیتی استفاده کنیم. به عنوان مثال می‌توانیم کل یک حافظه فلش و یا قسمتی از حجم آن را به یک گاوصندوق تبدیل کنیم و مطمئن باشیم که هیچ‌کس نمی‌تواند به صندوق ما دسترسی داشته باشد.

در ادامه می‌خواهیم گاوصندوقی را در یک حافظه فلش ایجاد کنیم. از پنجره اصلی نرم‌افزار روی گزینه Portable Safe کلیک می‌کنیم (تصویر ۵۴).



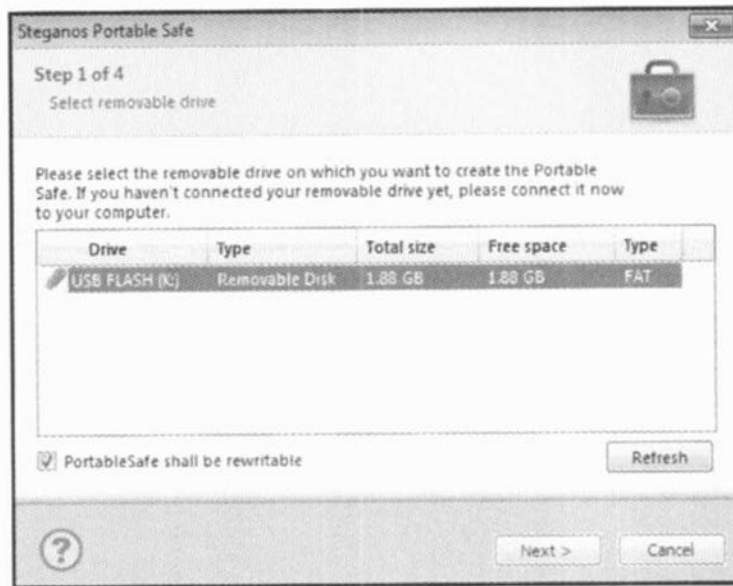
تصویر ۵۴

برای انتخاب حافظه فلش، در پنجره باز شده روی گزینه سمت راست کلیک می‌کنیم (تصویر ۵۵).



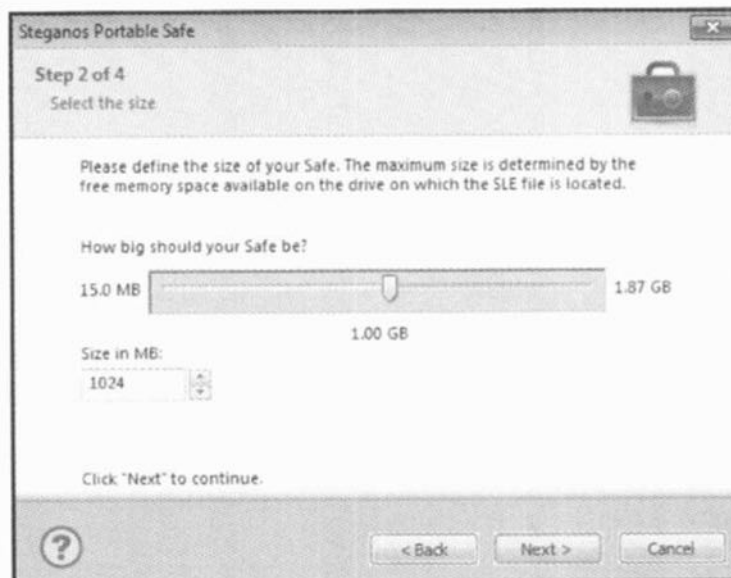
تصویر ۵۵

در پنجره بعدی حافظه فلشی که به رایانه متصل کرده‌ایم را از لیست انتخاب کرده و روی Next کلیک می‌کنیم (تصویر ۵۶).



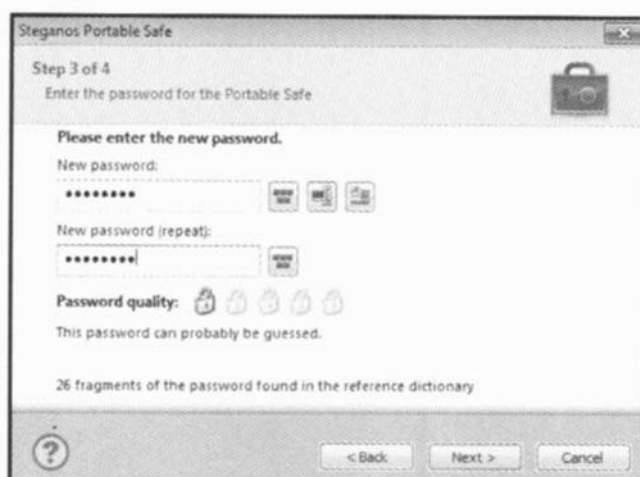
تصویر ۵۶

در پنجره بعدی حجم گاو صندوق را تعیین می کنیم. دقت داشته باشید حجم گاو صندوق را حداکثر به میزان فضای خالی حافظه فلش می توانیم قرار دهیم. ما حجم گاو صندوق را ۱ گیگا بایت انتخاب می کنیم (تصویر ۵۷).



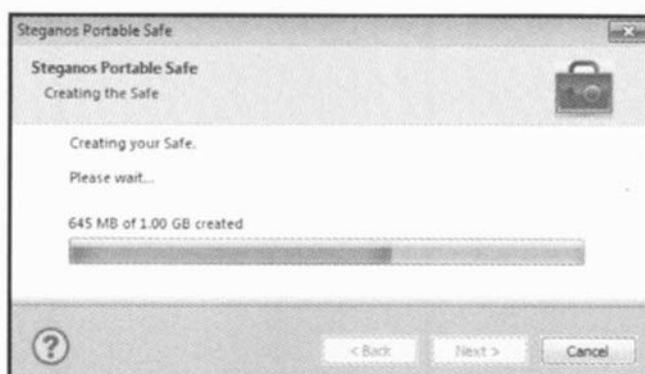
تصویر ۵۷

با کلیک روی **Next** وارد پنجره تعیین پسورد می شویم. در این پنجره پسوردی را وارد می کنیم (تصویر ۵۸).



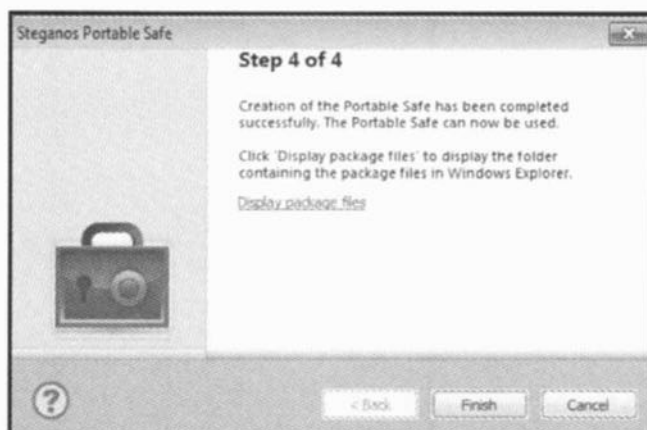
تصویر ۵۸

حال روی **Next** کلیک می‌کنیم و منتظر می‌مانیم تا این مرحله به پایان برسد (تصویر ۵۹).



تصویر ۵۹

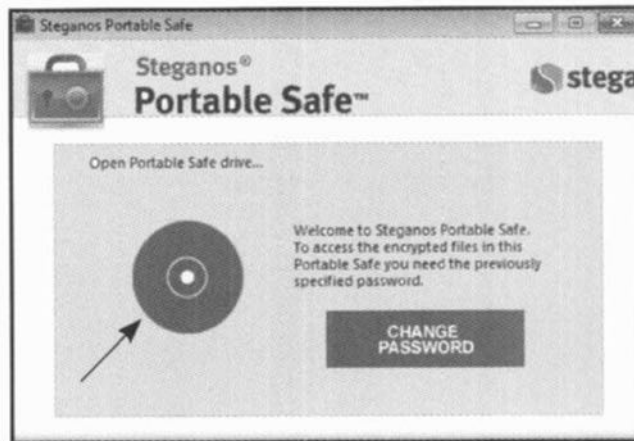
پس از پایان این مرحله روی دکمه **Finish** کلیک می‌کنیم (تصویر ۶۰).



تصویر ۶۰

هم اکنون یک گاو صندوق با حجم ۱ گیگابایت در حافظه فلش ما تولید شده است.

برای ورود به این گاو صندوق کافی است ابتدا وارد پوشه Portable_Safe در حافظه فلش بشویم. سپس روی فایل usbstarter.exe جفت کلیک می کنیم. با این کار پنجره‌ای باز می شود. در این پنجره روی آیکن Open Portable Safe drive کلیک می کنیم تا پنجره جدیدی باز شود (تصویر ۶۱).



تصویر ۶۱

اینجا روی دکمه OK کلیک می کنیم (تصویر ۶۲).



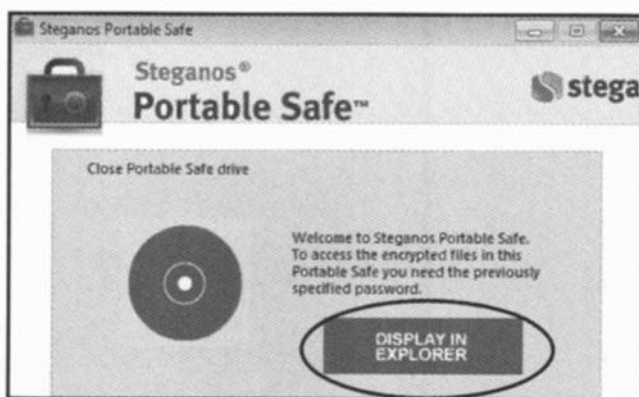
تصویر ۶۲

در پنجره بعدی پسورد این گاو صندوق را وارد کرده و سپس OK می کنیم (تصویر ۶۳).



تصویر ۶۳

حالا می‌توانیم با کلیک روی دکمه DISPLAY IN EXPLORER وارد گاوصندوق مان بشویم. با این کار پنجره گاوصندوق مثل یک درایو معمولی باز می‌شود (تصویر ۶۴).

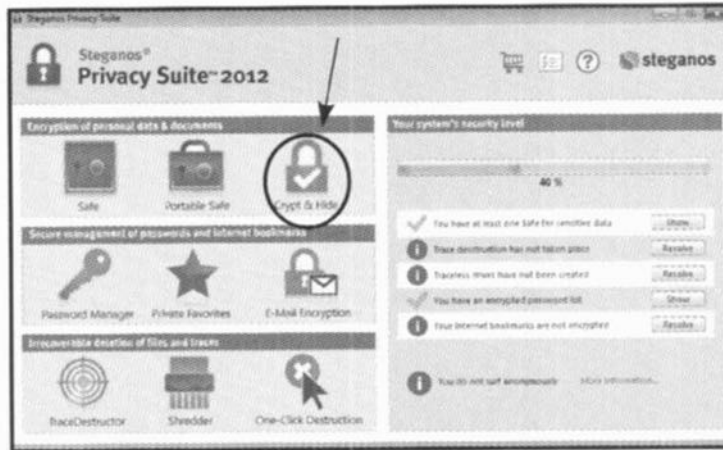


تصویر ۶۴

با بستن این پنجره نیز گاوصندوق، به طور خودکار بسته می‌شود.

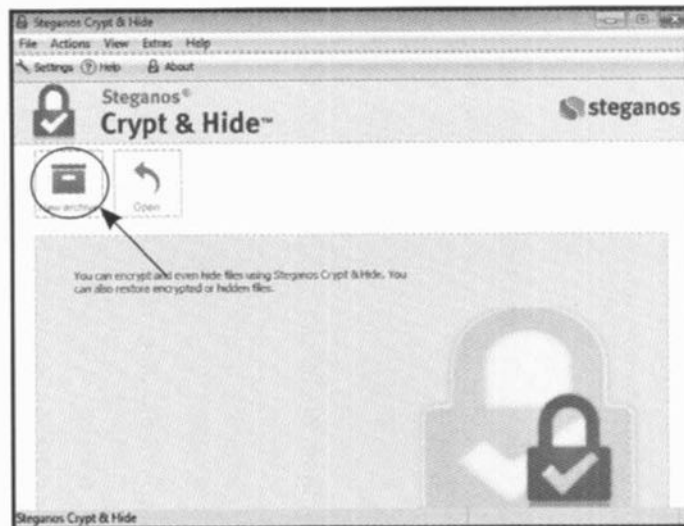
درس نهم: رمز گذاری روی فایل‌ها و پوشه‌ها

در این بخش می‌خواهیم برای دسترسی به فایل‌های محرمانه یک پسورد قرار بدهیم. تفاوت این کار با گاوصندوق این است که برای گاوصندوق یک حجم اولیه در نظر می‌گرفتیم و سپس اطلاعات را در داخل آن قرار می‌دادیم. اما در این بخش برای خود فایل‌ها یا پوشه‌ها پسورد می‌گذاریم. برای این کار از پنجره اصلی نرم‌افزار گزینه Crypt & Hide را انتخاب می‌کنیم (تصویر ۶۵).



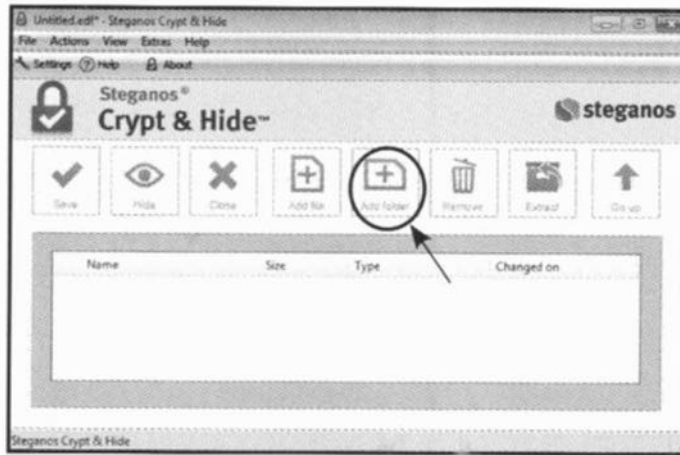
تصویر ۶۵

در پنجره باز شده روی گزینه **New archive** کلیک می‌کنیم تا پنجره مربوط به آن ظاهر شود (تصویر ۶۶).



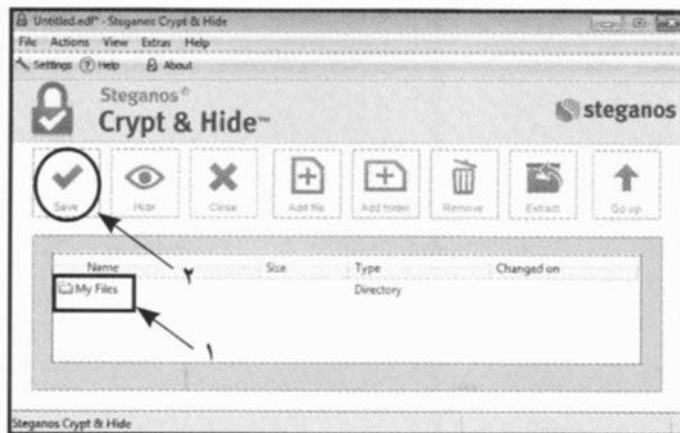
تصویر ۶۶

در پنجره بعد روی گزینه **Add folder** کلیک می‌کنیم تا پوشه‌ای که حاوی اطلاعات محرمانه ما می‌باشد را انتخاب کنیم (تصویر ۶۷).



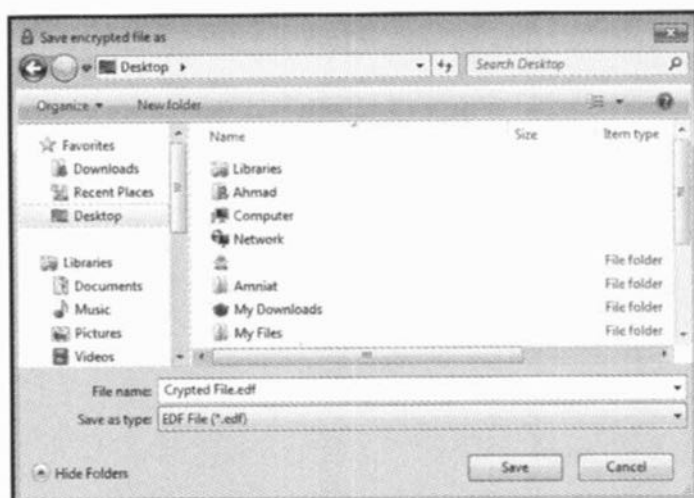
تصویر ۶۷

ما پوشه‌ای با نام **My Files** را که از قبل در دسکتاپ قرار داده‌ایم را انتخاب می‌کنیم (شماره ۱ در تصویر ۶۸). با این کار این پوشه به لیست این پنجره اضافه می‌شود. حالا برای رمز گذاری روی این پوشه، روی گزینه **Save** (شماره ۲ در تصویر ۶۸) کلیک می‌کنیم.



تصویر ۶۸

در پنجره باز شده مکان قرارگیری فایل تولیدی و هم چنین نام آن را انتخاب می‌کنیم. ما نام فایل امنیتی تولید شده را **Crypted File** می‌گذاریم و مکان ذخیره شدن آن را دسکتاپ انتخاب می‌کنیم. سپس روی دکمه **Save** کلیک می‌کنیم (تصویر ۶۹).



تصویر ۶۹

در پنجره بعدی پسورد مورد نظرمان را وارد کرده و سپس روی OK کلیک می‌کنیم (تصویر ۷۰).



تصویر ۷۰

پس از کمی انتظار و به پایان رسیدن عملیات پسورد گذاری، پوشه My Files در قالب فایل‌سی با نام Crypted File.edf در دسکتاپ ایجاد می‌شود که دارای پسورد نیز می‌باشد. البته پوشه My Files در جای خود قرار دارد و تغییری در آن ایجاد نمی‌شود. بنابراین بعد از اینکه از ایجاد فایل Crypted File.edf و درست کارکردن آن مطمئن شدیم می‌توانیم پوشه اصلی یعنی پوشه My Files را پاک کنیم.

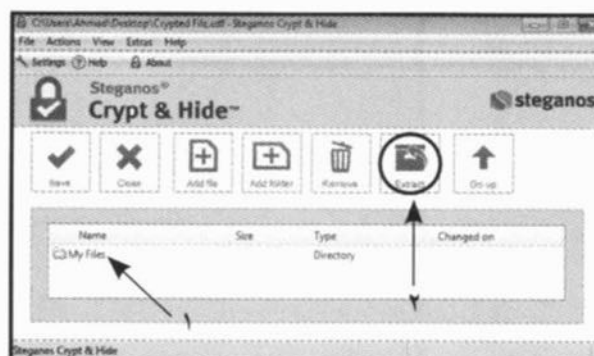
برای باز کردن و دسترسی به پوشه موجود در این فایل باید مراحل زیر را دنبال کنیم:

ابتدا روی فایل **Crypted File.edf** که در دسکتاپ قرار گرفته جفت کلیک می‌کنیم تا پنجره جدیدی باز شود (تصویر ۷۱).



تصویر ۷۱

در این پنجره پسورد فایل را وارد می‌کنیم و OK را کلیک می‌کنیم. مشاهده می‌کنیم که پوشه **My Files** در نرم‌افزار نمایش داده شده است. از همین مکان می‌توانیم به اطلاعات پوشه **My Files** دسترسی مستقیم داشته باشیم ولی اگر بخواهیم پوشه **My Files** را از حالت امنیتی به حالت اولیه و عادی خود برگردانیم کافی است ابتدا روی پوشه **My Files** (شماره ۱ در تصویر ۷۲) یک بار کلیک کنیم تا انتخاب شود و سپس روی گزینه **Extract** (شماره ۲ در تصویر ۷۲) کلیک کنیم.



تصویر ۷۲

در پنجره باز شده مکان ذخیره شدن این پوشه را انتخاب کرده و سپس روی دکمه OK کلیک می‌کنیم (تصویر ۷۳).



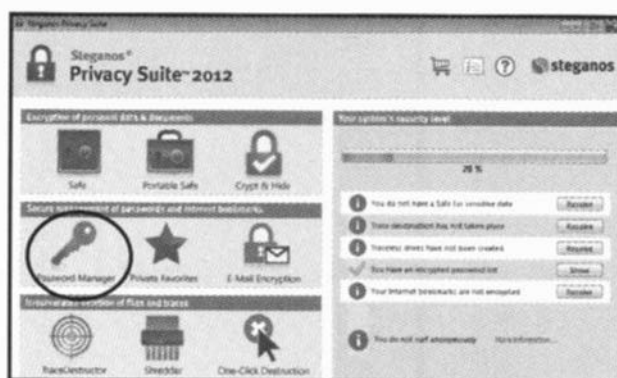
تصویر ۷۳

پس از کمی انتظار مشاهده می‌کنیم که پوشه My Files دوباره به دسکتاپ اضافه شده است.

درس دهم: مدیریت پسوردها

حتماً برایمان پیش آمده که در اثر انتخاب پسوردهای مختلف برای دسترسی به اطلاعات محرمانه و یا کارت‌های اعتباری و یا ایجاد حساب‌های کاربری مختلف در سایت‌ها و انجمن‌ها و هم چنین حساب‌های ایمیل گاهی اوقات آن‌ها را فراموش کنیم. شاید فکر کنیم انتخاب پسوردهای مشابه برای آن‌ها راه خوبی برای پیشگیری از فراموش کردن آن‌ها باشد ولی اگر کسی به پسورد شما دست یابد، می‌تواند همه اطلاعات شما را مشاهده کند یا احیاناً به شما آسیب بیشتری بزند. بهترین راه برای حل این مشکل استفاده از نرم‌افزارهای مدیریت پسورد می‌باشد که یکی از بهترین‌های آن در نرم‌افزار Steganos Privacy Suit موجود می‌باشد.

ما می‌توانیم پسوردهای خود را در این برنامه ذخیره کنیم و به جای این که همه پسوردها را به خاطر بسپاریم، فقط یک پسورد را برای ورود به این برنامه به یاد بسپاریم. با استفاده از همین یک پسورد می‌توانیم وارد این برنامه شده و به سایر پسوردها نیز دسترسی داشته باشیم. از قابلیت‌های دیگر این برنامه توانایی ذخیره اطلاعات حساب‌های بانکی و یا نام‌های کاربری می‌باشد. در ادامه روش کار با این برنامه را می‌آموزیم. برای دسترسی به این برنامه در پنجره اصلی نرم‌افزار روی قسمت Password Manager کلیک می‌کنیم (تصویر ۷۴).



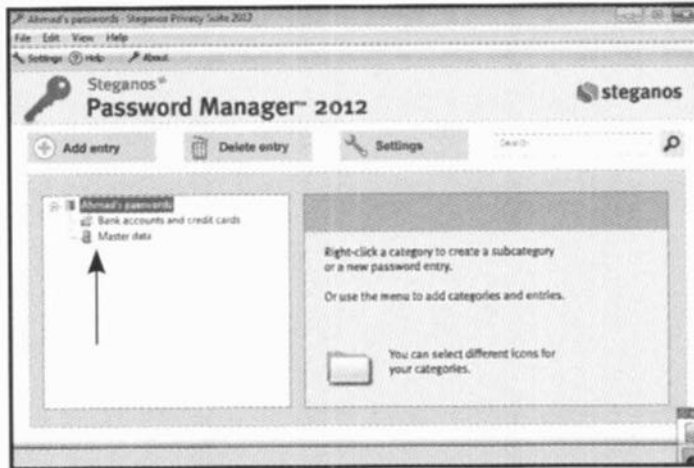
تصویر ۷۴

پنجره‌ای باز می‌شود که در آن پسوردی را برای ورود به این قسمت تعیین می‌کنیم (تصویر ۷۵).



تصویر ۷۵

با کلیک روی دکمه OK وارد صفحه مدیریت پسورد می شویم
(تصویر ۷۶).



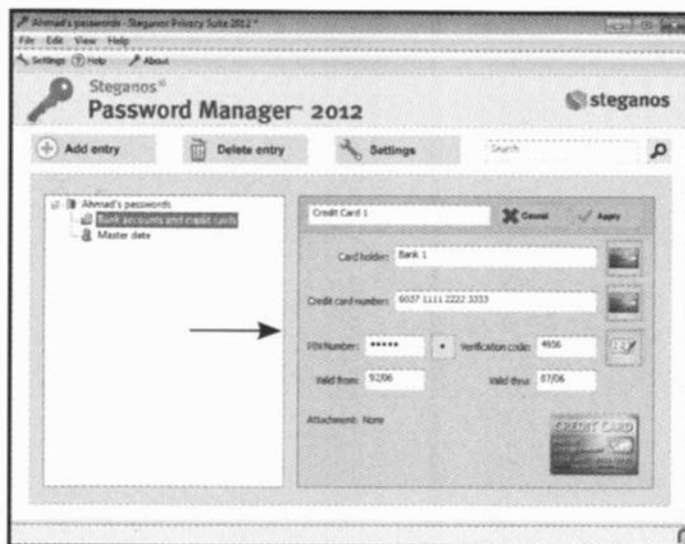
تصویر ۷۶

در شاخه Ahmad's passwords (Ahmad نام یوزر ویندوز می باشد) که تمامی زیرشاخه‌ها و پسوردها در آن قرار می‌گیرد دو گزینه وجود دارد:
۱- Bank accounts and credit cards: با کلیک روی این گزینه می‌توانیم اطلاعات بانکی و شماره حساب و رمز کارت‌های اعتباری را ذخیره کنیم. به عنوان مثال برای ثبت اطلاعات کارت‌های بانکی با راست کلیک روی این قسمت، گزینه Add credit card را انتخاب می‌کنیم (تصویر ۷۷).



تصویر ۷۷

با این کار، کادرهایی برای وارد کردن این اطلاعات در سمت راست پنجره، ظاهر می‌شود. ما اطلاعات مربوط به کارت بانکی را در آن ثبت کرده و سپس روی دکمه Apply کلیک می‌کنیم (تصویر ۷۸).



تصویر ۷۸

این کار را برای ۲ کارت بانکی دیگر نیز انجام می‌دهیم. مشاهده می‌کنیم این ۳ کارت در زیرشاخه Bank account and credit cards اضافه شده‌اند (تصویر ۷۹).



تصویر ۷۹

۲- Master data: با کلیک روی این قسمت می‌توانیم اطلاعات شخصی خودمان از قبیل نام، آدرس، شماره تلفن، ایمیل و... را ذخیره کنیم. برای ذخیره پسوردها در این نرم‌افزار بهتر است ابتدا یک مجموعه خاص را برای آن پسوردها ایجاد کنیم. مثلاً برای ذخیره پسوردهایی که روی فایل‌ها و فولدرها قرار داده‌ایم، مجموعه‌ای با نام Passwords ایجاد می‌کنیم و آن پسوردها را در این مجموعه ثبت می‌کنیم؛ و یا برای ذخیره حساب‌های کاربری که در سایت‌های اینترنتی ایجاد کرده‌ایم مجموعه‌ای با نام Internet Accounts ایجاد می‌کنیم و همچنین برای ذخیره پسورد و نام کاربری ایمیل‌هایمان مجموعه Emails را می‌سازیم. برای اضافه کردن یک مجموعه ابتدا روی قسمت Ahmad's Passwords راست کلیک کرده و از منوی باز شده گزینه Add new category را انتخاب می‌کنیم (تصویر ۸۰).



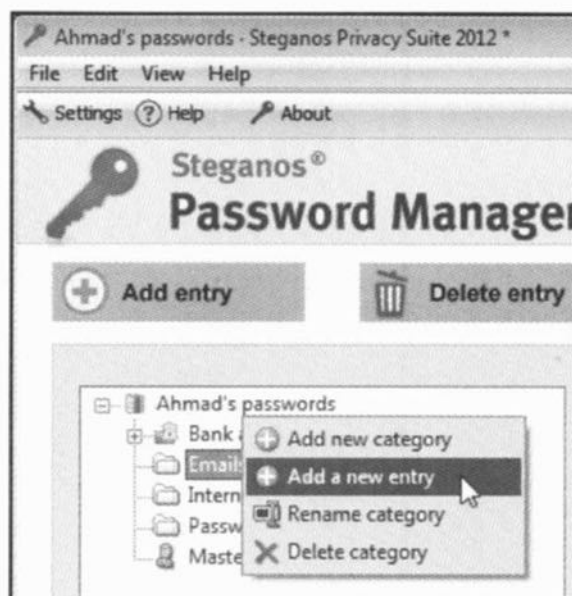
تصویر ۸۰

در پنجره باز شده نام مجموعه را وارد می‌کنیم. ما از این طریق ۳ مجموعه Passwords و Internet Accounts و Emails را ایجاد می‌کنیم. با این کار این ۳ مجموعه به شاخه Ahmad's passwords اضافه می‌شوند (تصویر ۸۱).




تصویر ۸۱

حال با راست کلیک روی یکی از این مجموعه‌ها و انتخاب گزینه Add a new entry می‌توانیم اطلاعات و پسوردها را ثبت و ذخیره کنیم. ما برای نمونه می‌خواهیم اطلاعات یک ایمیل را ذخیره کنیم. برای این کار روی مجموعه Emails راست کلیک کرده و از منوی باز شده گزینه Add a new entry را انتخاب می‌کنیم (تصویر ۸۲).



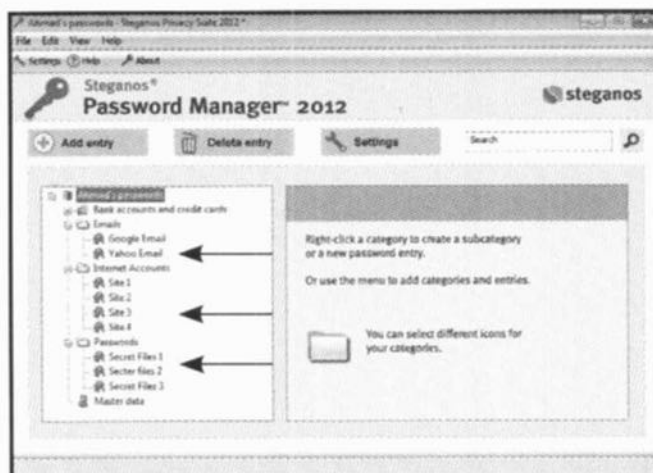
تصویر ۸۲

حالا در قسمت راست پنجره، اطلاعات مربوط به این حساب ایمیل را وارد می‌کنیم. (تصویر ۸۳) همچنین با کلیک روی دکمه  می‌توانیم کاراکترهای پسوردمان را مشاهده کنیم.



تصویر ۸۳

با کلیک روی دکمه Apply اطلاعاتی که وارد کردیم ذخیره شده و به زیرشاخه Emails اضافه می‌شود. به همین ترتیب می‌توانیم سایر پسوردها و حساب‌های کاربری خود را در مجموعه‌های مناسب ثبت و ذخیره کنیم (تصویر ۸۴).

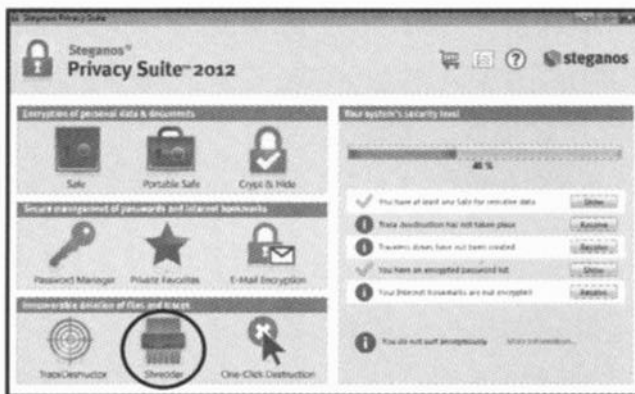


تصویر ۸۴

درس یازدهم: پاکسازی غیر قابل بازیابی اطلاعات

ممکن است برای شما پیش آمده باشد که خواسته باشید فایل‌ها و یا اسنادی را از روی سیستم‌تان به نحوی پاک کنید که دیگر افراد نتوانند به هیچ وجه به آن‌ها دسترسی یابند یا با استفاده از نرم‌افزارهای بازیابی، آن‌ها را برگردانده و از آن‌ها استفاده نمایند. معمولاً وقتی می‌خواهیم رایانه خود را بفروشیم و یا این که آن را برای تعمیر به دست افراد غریبه بسپاریم لازم است این کار را انجام دهیم.

می‌دانیم که با پاک کردن ساده و یا فرمت کردن هارد اطلاعات آن از بین نمی‌رود. نرم‌افزار Steganos Privacy Suit این قابلیت را دارد که هر فایل

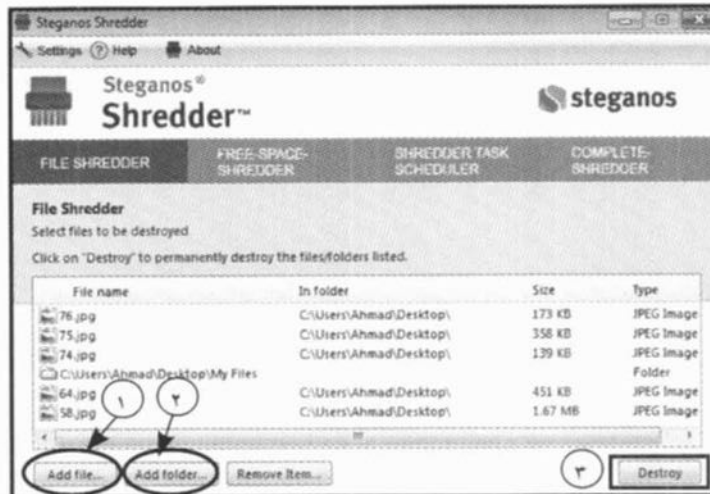


تصویر ۸۵

که بخواهیم از شرش خلاص شویم را به کل نابود کند و کاری کند که دیگر قابل برگشت نباشد. برای انجام این کار مراحل زیر را پیگیری می‌کنیم: از پنجره اصلی نرم‌افزار

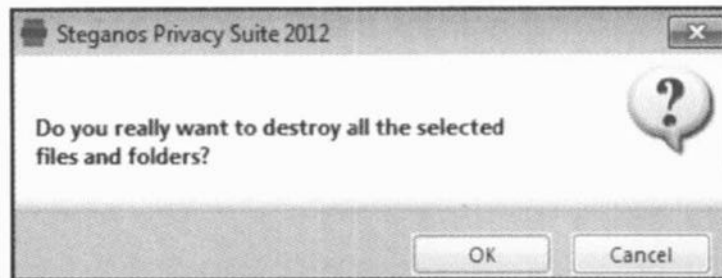
گزینه Shredder را انتخاب می‌کنیم (تصویر ۸۵).

در پنجره باز شده با کلیک روی دکمه Add folder (شماره ۲ در تصویر ۸۶) می‌توانیم پوشه‌ای را که می‌خواهیم پاک کنیم انتخاب کنیم. همچنین اگر بخواهیم چند فایل را که در پوشه‌های مختلف قرار دارند پاک کنیم می‌توانیم روی دکمه Add file (شماره ۱ در تصویر ۸۶) کلیک کنیم.



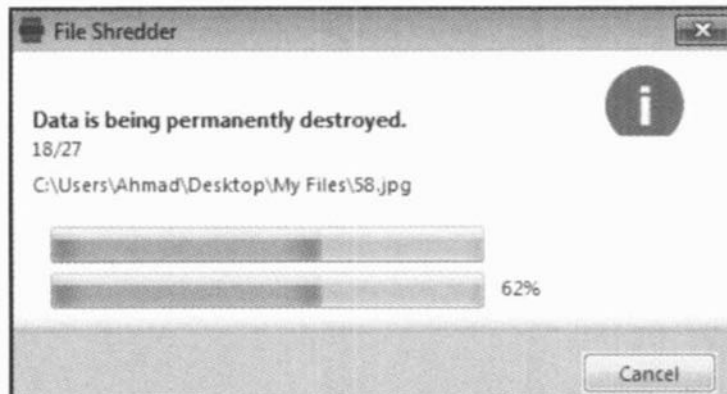
تصویر ۸۶

پس از انتخاب و اضافه کردن فایل‌ها و پوشه‌های مورد نظر به لیست روی دکمه Destroy (شماره ۳ در تصویر ۸۶) کلیک می‌کنیم. سپس در پنجره باز شده گزینه OK را انتخاب می‌کنیم (تصویر ۸۷).



تصویر ۸۷

حالا آن قدر صبر می‌کنیم تا عملیات پاکسازی به پایان برسد و پس از آن روی دکمه OK کلیک می‌کنیم (تصویر ۸۸).



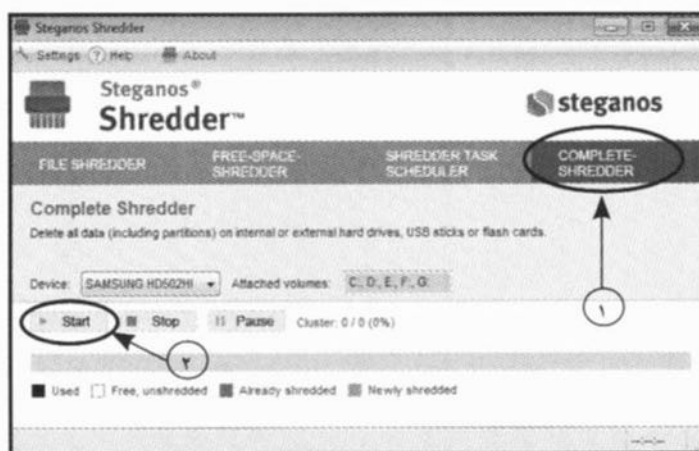
تصویر ۸۸

با این کار تمام اطلاعاتی که انتخاب کرده بودیم از هارد دیسک حذف فیزیکی شدند یعنی دیگر قابل بازیابی نیستند.

نکته ...

حتماً به این نکته توجه داشته باشید که زمانی به حذف فیزیکی اطلاعات می‌پردازیم که مطمئن باشیم دیگر به آن اطلاعات هیچ نیازی نداریم. چون این کار، اطلاعات مورد نظر را برای همیشه نابود می‌کند. پس عجله در این کار، نتیجه‌ای جز پشیمانی برای شما نخواهد داشت.

برای پاکسازی کل هارد دیسک می‌توانیم به سربرگ COMPLETE SHREDDER (شماره ۱ در تصویر ۸۹) در پنجره Shredder برویم.



تصویر ۸۹

سپس با انتخاب گزینه Start (شماره ۲ در تصویر ۸۹) تمام اطلاعات موجود در هارد دیسک پاک می‌شوند.

نکته ...

دقت داشته باشید که انجام این عمل یعنی پاکسازی کل هارد دیسک را فقط زمانی انجام دهید که از این کار اطمینان کامل دارید زیرا با این کار تمام فایل‌های ما از بین می‌روند و دیگر قابل برگشت نیستند.

ما در این فصل امکاناتی از نرم‌افزار Steganos Privacy Suit که بیشتر کاربرد دارند را معرفی کرده و آموزش دادیم. این نرم‌افزار امکانات و ویژگی‌های دیگری نیز دارد که آموزش آن‌ها در فضای این کتاب نمی‌گنجد. به همین دلیل در ادامه چند تا از این امکانات را نام می‌بریم:

ارسال ایمیل کد گذاری شده در قسمت E-Mail Encryption

پاکسازی مسیرهای طی شده در وب سایت‌های اینترنتی و هم چنین ویندوز در قسمت Trace Destructor

پاکسازی کوکی‌ها و کش و... مربوط به مرورگرها به منظور جلوگیری از سوءاستفاده‌های اینترنتی در قسمت Trace Destructor و ...

فصل دوم

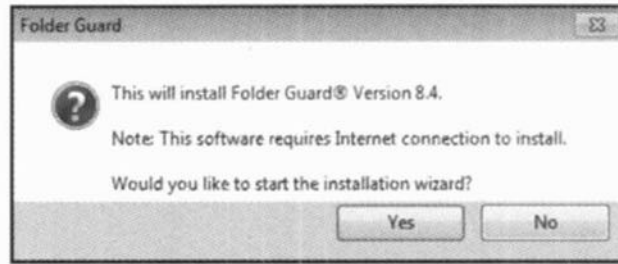
نرم افزار Folder Guard

نرم افزار Folder Guard را می توان یکی از قدرتمندترین نرم افزارهای قفل گذاری بر روی فولدرها دانست. این نرم افزار با توجه به حجم کم، کاربرد آسان و امنیت بالایی که دارد می تواند ابزار خوبی برای قرار دادن پسورد بر روی پوشه های ما باشد. در این نرم افزار ما ابتدا یک پسورد اصلی یا Master Password برای ورود به نرم افزار قرار می دهیم، سپس بر روی هر پوشه ای که بخواهیم جداگانه پسوردی را تنظیم می کنیم تا به هنگام دسترسی به فولدر مورد نظر از کاربر درخواست پسورد شود. البته تمام روش هایی که در این فصل برای کنترل پوشه ها ارائه خواهند شد را می توان روی درایوها نیز انجام داد.

ما با این نرم افزار قدرتمند می توانیم بر روی پوشه های خود کنترل کاملی داشته باشیم و سطح امنیت هر کدام از آنها را به سلیقه خودمان مخفی، فقط خواندنی و یا غیر قابل دسترس قرار دهیم. همچنین ما می توانیم کنترل کامل بر روی تمامی برنامه های ویندوز مانند کنترل پنل، استارت منو، سرچ ویندوز، RUN داشته باشیم و مخفی سازی درایوها و همچنین غیر قابل دسترس کردن floppy, CD-ROM و... را انجام دهیم.

درس اول: نصب نرم افزار Folder Guard

ابتدا فایل folder guard.exe را اجرا می کنیم. در پنجره باز شده روی Yes کلیک می کنیم (تصویر ۹۰).



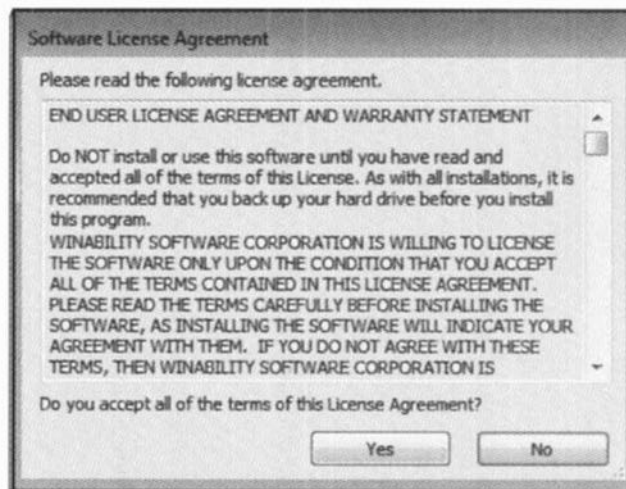
تصویر ۹۰

در پنجره بعدی Next را کلیک می‌کنیم تا به مرحله بعد برویم (تصویر ۹۱).



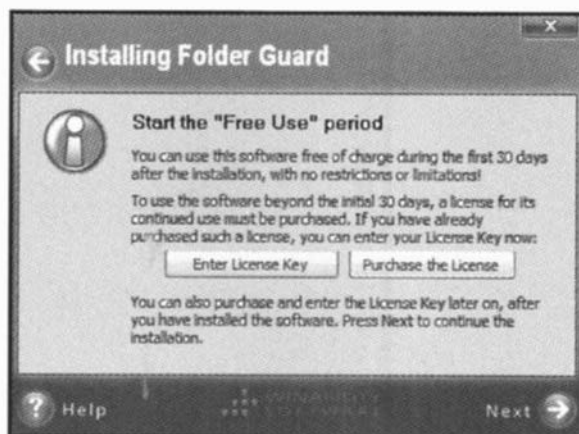
تصویر ۹۱

در اینجا نیز روی دکمه Yes کلیک می‌کنیم (تصویر ۹۲).



تصویر ۹۲

باز هم Next را کلیک می‌کنیم (تصویر ۹۳).



تصویر ۹۳

در پنجره بعدی می‌توانیم محل نصب شدن نرم‌افزار را تعیین کنیم. همان‌طور که در تصویر ۹۴ مشاهده می‌کنیم مسیر `C:\Program Files\Folder Guard` به‌طور پیش‌فرض انتخاب شده است. ما تغییری در این قسمت نمی‌دهیم و روی **Next** کلیک می‌کنیم.



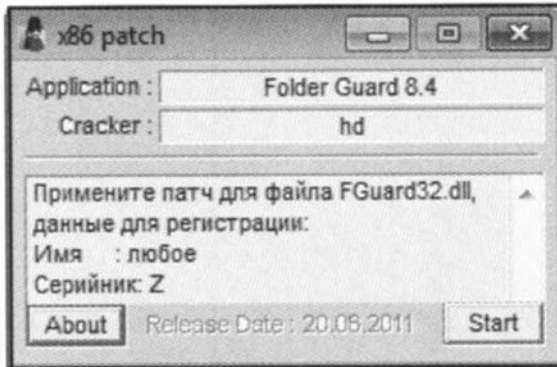
تصویر ۹۴

در پنجره‌های بعدی نیز روی **Next** کلیک می‌کنیم تا عملیات نصب به پایان برسد.

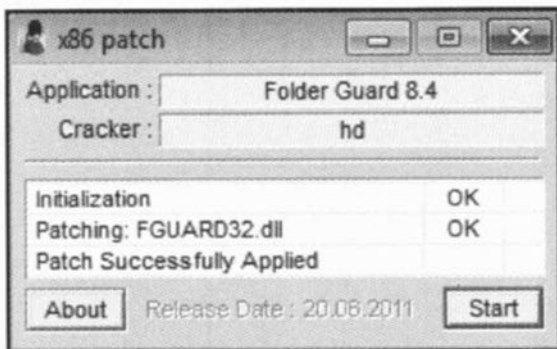
حالا نرم‌افزار Folder Guard در رایانه ما نصب شده است ولی به صورت موقتی یعنی ۳۰ روزه می‌باشد. برای دائمی کردن این نرم‌افزار مراحل زیر را انجام می‌دهیم. ابتدا اگر نرم‌افزار folder guard را اجرا کرده‌ایم

آن را به طور کامل می‌بندیم. سپس پوشه Crack موجود در پوشه نصب این نرم‌افزار را باز می‌کنیم. در این پوشه دو فایل به نام‌های x64.patch.exe و x86.patch.exe وجود دارد.

اگر ویندوز رایانه ما از نوع ۳۲ بیتی باشد از فایل x86.patch.exe استفاده می‌کنیم و اگر ویندوز ما ۶۴ بیتی باشد از فایل x64.patch.exe استفاده می‌کنیم. ویندوزی که من از آن استفاده می‌کنم ۳۲ بیتی می‌باشد. در نتیجه فایل x86.patch.exe را در محل نصب نرم‌افزار یعنی C:\Program Files\Folder Guard



تصویر ۹۵



تصویر ۹۶

و یا ویستا باشد روی این فایل راست کلیک می‌کنیم و گزینه Run as administrator را انتخاب می‌کنیم ولی اگر ویندوز ما XP باشد روی این فایل فقط جفت کلیک می‌کنیم تا پنجره مربوطه باز شود (تصویر ۹۵).

در این پنجره روی دکمه Start کلیک می‌کنیم و صبر می‌کنیم تا پیغام OK نمایش داده شود (تصویر ۹۶).

حال این پنجره را بسته و یکبار ویندوز را ریست می‌کنیم. بعد از

اجرای دوباره ویندوز، نرم‌افزار Folder Guard را با کلیک روی آیکن این نرم‌افزار از روی دسکتاپ اجرا می‌کنیم.

با این کار پنجره‌ای باز می‌شود که از ما می‌خواهد شماره سریال نرم‌افزار را وارد کنیم (تصویر ۹۷).



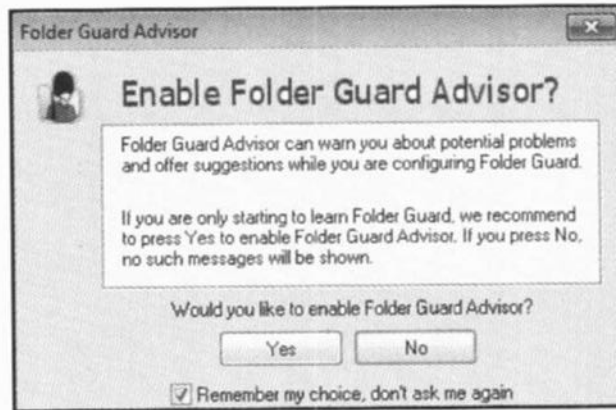
تصویر ۹۷

ما روی دکمه Enter License Key کلیک می‌کنیم و در پنجره ظاهر شده گزینه Yes را انتخاب می‌کنیم تا پنجره Enter License Key باز شود (تصویر ۹۸).



تصویر ۹۸

در این پنجره در قسمت Licensed To عبارت SoftGozar.com را وارد می‌کنیم. در قسمت بعدی عدد ۱ را وارد می‌کنیم و در قسمت آخر حرف Z بزرگ را وارد می‌کنیم. حال روی دکمه Continue کلیک می‌کنیم تا پنجره Folder Guard Advisor ظاهر شود (تصویر ۹۹).



تصویر ۹۹

نرم‌افزار Folder Guard این قابلیت را دارد که در حین انجام کارهای مختلف با این نرم‌افزار نکته‌هایی را یادآوری کند تا اشتباهات کاربر را به حداقل برساند. اگر بخواهیم این قابلیت را فعال کنیم می‌توانیم روی Yes کلیک کنیم در غیر این صورت باید روی دکمه No کلیک کنیم. ما نیز همین گزینه را انتخاب کرده و به مرحله بعد می‌رویم. بعد از این کار پنجره‌ای ظاهر می‌شود که با کلیک روی دکمه OK پنجره Master Password نمایش داده می‌شود (تصویر ۱۰۰).



تصویر ۱۰۰

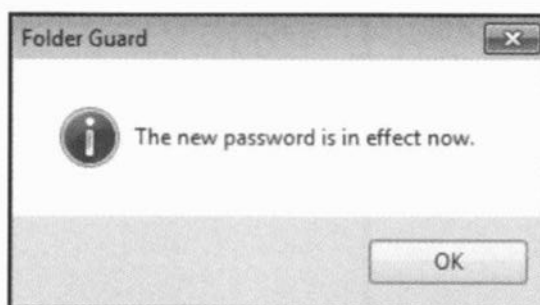
در این پنجره باید یک Master Password یا همان پسورد اصلی برای نرم‌افزار تعیین کنیم. از این پسورد در زمان وارد شدن به محیط این نرم‌افزار و یا اعمال تغییرات در آن و یا پاک کردن این نرم‌افزار از ویندوز استفاده

می‌شود. در واقع کسی که پسورد اصلی نرم‌افزار را نداند نمی‌تواند وارد محیط کاربری آن شود و در دسترسی به اطلاعات، تغییری ایجاد کند. در قسمت **New Password** پسورد مورد نظرمان را وارد می‌کنیم. در قسمت **Confirm New Password** نیز پسورد وارد شده در قسمت قبل را دوباره وارد می‌کنیم تا نرم‌افزار مطمئن شود پسورد خود را درست نوشته‌ایم (تصویر ۱۰۱).



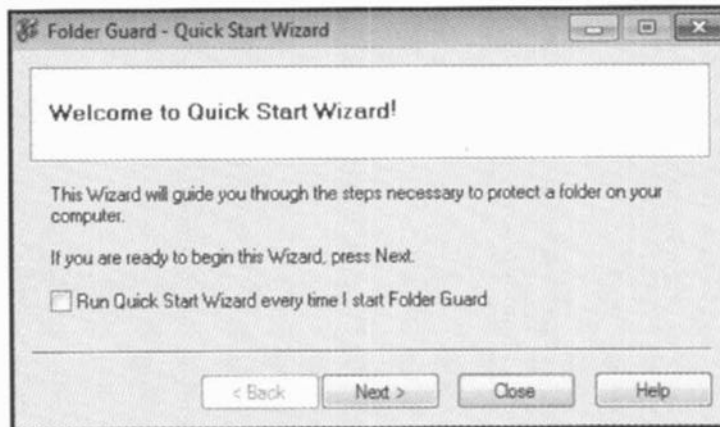
تصویر ۱۰۱

حالا روی دکمه **OK** کلیک می‌کنیم تا پنجره تایید نمایش داده شود (تصویر ۱۰۲).



تصویر ۱۰۲

با کلیک روی **OK** پنجره **Quick Start Wizard** ظاهر می‌شود. در این پنجره گزینه **Run Quick Start Wizard every time** را غیرفعال کرده و روی دکمه **Close** کلیک می‌کنیم (تصویر ۱۰۳).



تصویر ۱۰۳

تا اینجا مراحل نصب نرم افزار Folder Guard و انتخاب پسورد اصلی این نرم افزار به پایان رسیده است. در ادامه با محیط این نرم افزار و قابلیت های آن آشنا خواهیم شد.

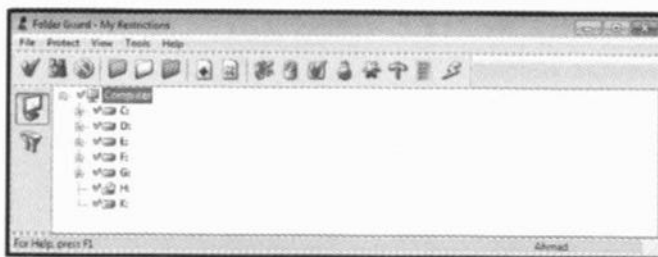
درس دوم: تنظیم نوع دسترسی به یک پوشه

در این بخش می خواهیم بر روی یک پوشه که حاوی اطلاعات خصوصی است محدودیت ایجاد کنیم. نرم افزار Folder Guard این اجازه را به ما می دهد که بتوانیم محتویات پوشه ای را غیر قابل دسترس و یا فقط خواندنی کنیم. برای این کار از روی دسکتاپ روی آیکن Folder Guard جفت کلیک و آن را اجرا می کنیم. پنجره ای باز می شود که ما پسورد اصلی نرم افزار را در آن وارد کرده و سپس روی دکمه OK کلیک می کنیم (تصویر ۱۰۴).



تصویر ۱۰۴

پنجره اصلی نرم افزار ظاهر می شود (تصویر ۱۰۵).

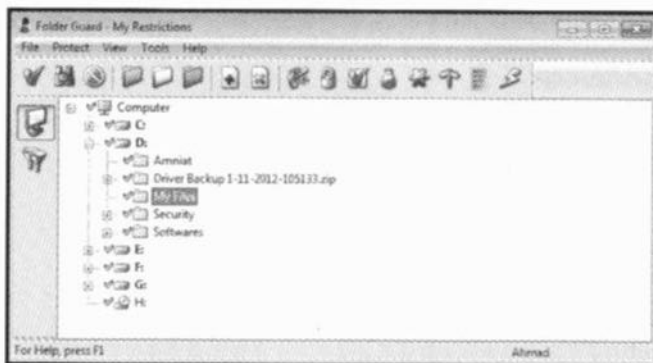


تصویر ۱۰۵

ما پوشه‌ای با نام My Files را که حاوی یک سری اطلاعات شخصی می باشد در درایو D سیستم ایجاد کرده ایم. حال می خواهیم نوع دسترسی به این پوشه را تعیین کنیم.

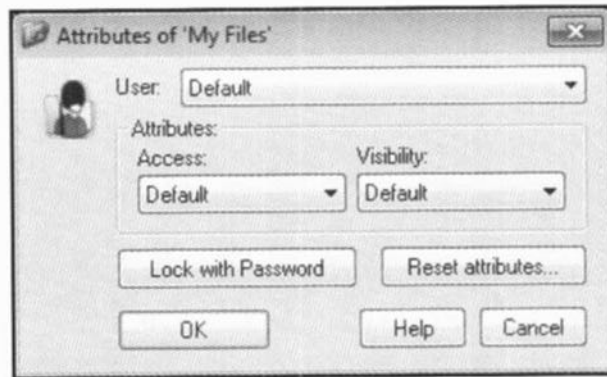
ابتدا باید وارد پنجره تنظیمات پوشه مورد نظر شویم. برای این کار مراحل زیر را دنبال می کنیم:

برای نمایش محتویات درایو D سیستم، روی علامت + در کنار آن کلیک می کنیم (تصویر ۱۰۶).



تصویر ۱۰۶

سپس روی پوشه My Files که قبلاً آن را در درایو D ایجاد کرده ایم جفت کلیک می کنیم تا پنجره تنظیمات آن باز شود (تصویر ۱۰۷).

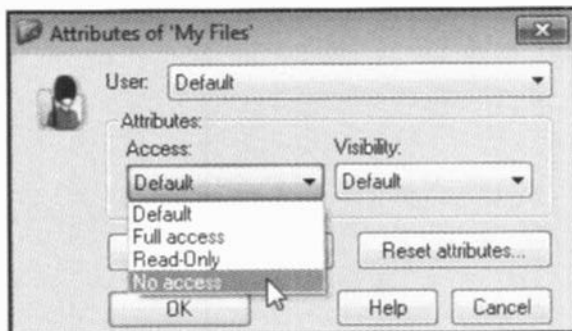


تصویر ۱۰۷

در این پنجره در قسمت User می‌توانیم محدودیت‌ها را برای کاربران دیگری که با یوزرهای متفاوت از این رایانه استفاده می‌کنند ایجاد کنیم. برای این کار کفایت روی دکمه Default کلیک کنیم تا لیست یوزرهای موجود در رایانه ما نمایش داده شود. سپس می‌توانیم یوزر مورد نظرمان را انتخاب کنیم. در قسمت Access چهار گزینه وجود دارد که انتخاب هر کدام از آنها نتایج زیر را به دنبال دارد:

۱- Default: هیچ تغییری در نوع دسترسی به پوشه مورد نظر ایجاد نمی‌کند.
 ۲- Full access: هیچ محدودیتی در دسترسی به این پوشه ایجاد نخواهد شد.

۳- Read-Only: باعث می‌شود دسترسی به پوشه مورد نظر از نوع فقط خواندنی شود. یعنی نمی‌توان هیچ تغییری در محتویات پوشه ایجاد کرد.
 ۴- No access: اجازه هیچ گونه دسترسی به محتویات پوشه را نمی‌دهد ولی




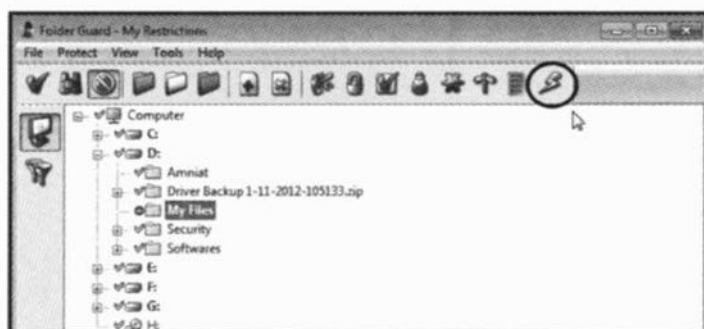
پوشه در حالت نمایان باقی می‌ماند. ما برای نمونه گزینه No access را انتخاب می‌کنیم و سپس روی OK کلیک می‌کنیم (تصویر ۱۰۸).

تصویر ۱۰۸

پس از زدن دکمه OK دوباره به پنجره اصلی نرم افزار هدایت می شویم. ما با انتخاب No access به نرم افزار دستور دادیم که دسترسی دیگران را به پوشه My Files قطع کند، ولی این دستور هنوز عملی نشده است. برای اجرای این دستور دو راه داریم:

۱- راه اول:

در پنجره اصلی نرم افزار روی دکمه  که Toggle Protection نام دارد کلیک می کنیم (تصویر ۱۰۹).

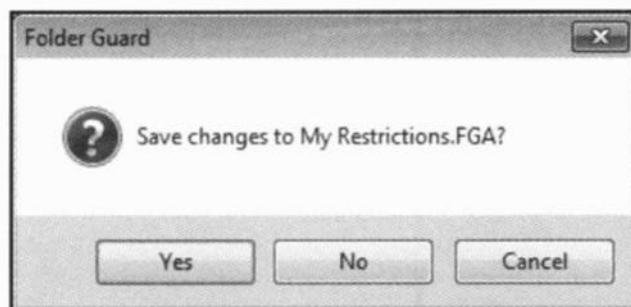


تصویر ۱۰۹

تا وقتی که این دکمه در حالت فشرده شده قرار داشته باشد نرم افزار Folder Guard دستورات را اعمال می کند.

۲- راه دوم:

ابتدا نرم افزار را می بندیم. با این کار پنجره ای نمایان می شود. در این پنجره گزینه Yes را انتخاب می کنیم (تصویر ۱۱۰).



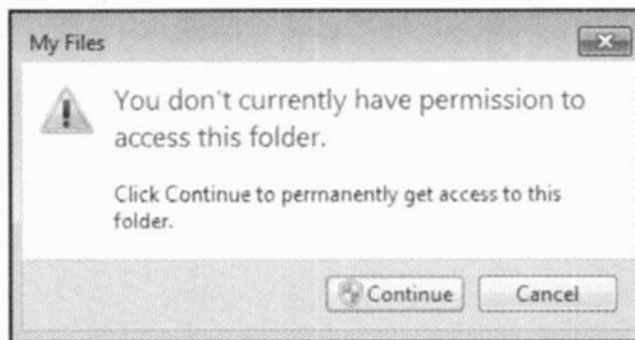
تصویر ۱۱۰

سپس پنجره دیگری با پیغام «آیا می‌خواهید نرم‌افزار Folder Guard محافظت از اطلاعات شما را آغاز کند؟» ظاهر می‌شود که ما روی دکمه Yes کلیک می‌کنیم (تصویر ۱۱۱).



تصویر ۱۱۱

ما راه اول را انتخاب می‌کنیم تا دستور No access روی پوشه مورد نظر اعمال شود. سپس از طریق My Computer وارد درایو D می‌شویم. با جفت کلیک روی پوشه My Files پنجره‌ای با پیغام «شما اجازه دسترسی به این پوشه را ندارید» نمایش داده می‌شود (تصویر ۱۱۲).



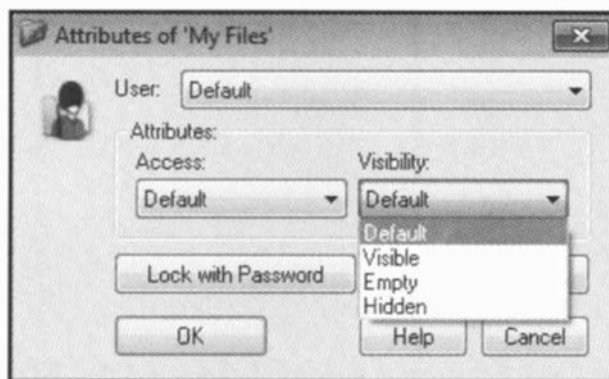
تصویر ۱۱۲

درس سوم: تنظیم نحوه نمایش اطلاعات یک پوشه

در این بخش می‌خواهیم در نحوه نمایش محتویات یک پوشه تغییراتی ایجاد کنیم که افراد غیر مجاز با دیدن آن تصور کنند این پوشه خالی می‌باشد و یا این که اصلاً نتوانند پوشه مورد نظر را ببینند.

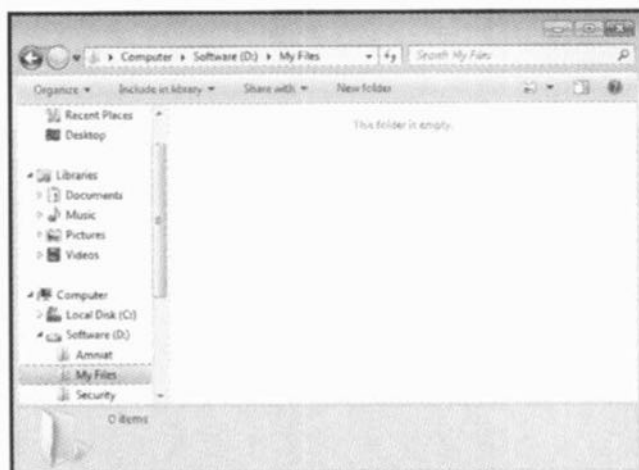
برای کار ابتدا به پنجره تنظیمات پوشه مورد نظرمان که My Files نام دارد می‌رویم.

در قسمت Visibility چهار گزینه وجود دارد که انتخاب هر یک از آنها نتایج زیر را به دنبال دارد (تصویر ۱۱۳).



تصویر ۱۱۳

- ۱- Default: هیچ تغییر در نحوه نمایش پوشه ایجاد نمی‌کند.
 - ۲- Visible: پوشه را قابل رؤیت می‌کند.
 - ۳- Empty: باعث می‌شود پوشه مورد نظر، خالی به نظر بیاید و هم چنین سائز آن را صفر کیلو بایت قرار می‌دهد.
 - ۴- Hidden: باعث می‌شود پوشه مورد نظر کلاً ناپدید و غیر قابل رؤیت شود.
- ما برای مثال گزینه Empty را انتخاب می‌کنیم و سپس روی OK کلیک می‌کنیم.
- برای این که این دستور اجرا شود در پنجره اصلی نرم‌افزار با کلیک روی دکمه Toggle Protection آن را در حالت فشرده شده و فعال قرار می‌دهیم.
- حال از طریق My Computer به درایو D رفته و سپس وارد پوشه My Files می‌شویم (تصویر ۱۱۴).



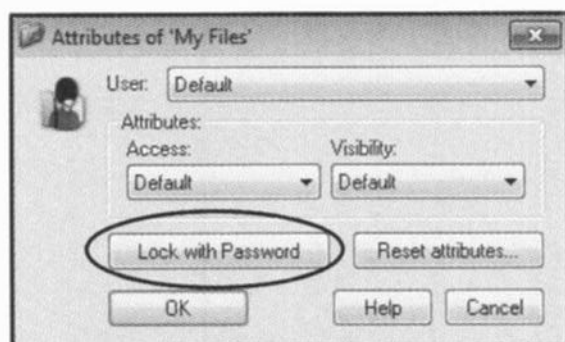
تصویر ۱۱۴

می بینیم که محتویات پوشه ما ناپدید شده‌اند و در ظاهر هیچ اطلاعاتی در آن وجود ندارد.

درس چهارم: قرار دادن پسورد برای دستیابی به یک پوشه

در این بخش می خواهیم کاری کنیم که نرم افزار برای دیدن محتویات یک پوشه از ما پسورد بخواهد. در واقع فقط کاربرانی قادر به ورود به این پوشه خواهند بود که از این پسورد آگاه باشند.

ما می خواهیم این عمل را بر روی پوشه My Files که در درایو D قرار دارد انجام دهیم.



تصویر ۱۱۵

برای این کار ابتدا از طریق نرم افزار پنجره تنظیمات این پوشه را باز می کنیم. سپس روی دکمه Lock with Password کلیک

می کنیم (تصویر ۱۱۵).



تصویر ۱۱۶

در پنجره باز شده در قسمت **New Password** پسورد موردنظرمان را وارد می‌کنیم. در قسمت **Confirm New Password** همان پسورد را دوباره تکرار می‌کنیم. در این پنجره و سپس در پنجره تنظیمات روی **OK** کلیک می‌کنیم (تصویر ۱۱۶).

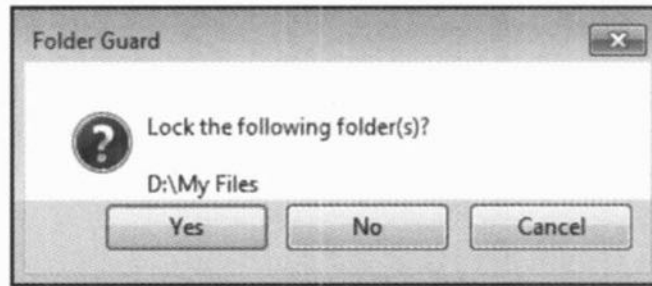


تصویر ۱۱۷

حالا در پنجره اصلی روی دکمه **Toggle Protection** کلیک می‌کنیم تا نرم‌افزار به حالت فعال درآید. بعد از این مراحل از طریق **My Computer** وارد درایو **D** شده و روی پوشه **My Files** جفت کلیک

می‌کنیم. کادری باز می‌شود و از ما پسورد دسترسی به این پوشه را می‌خواهد (تصویر ۱۱۷).

پسوردی که برای این پوشه انتخاب کرده بودیم را وارد کرده و سپس روی **OK** کلیک می‌کنیم. پس از آن پوشه **My Files** باز می‌شود. وقتی کارمان با این پوشه به پایان رسید با بستن این پوشه پنجره‌ای ظاهر می‌شود که با کلیک روی گزینه **Yes** این پوشه دوباره به حالت قفل شده بر می‌گردد (تصویر ۱۱۸).



تصویر ۱۱۸

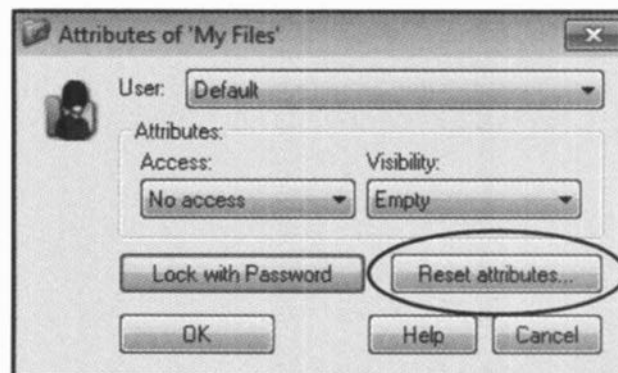
نکته ...

در نرم افزار Folder Guard می توانیم تمام روش های ارائه شده در درس های دوم، سوم و چهارم را به طور همزمان نیز روی پوشه ها اعمال کنیم. یعنی به عنوان مثال می توانیم یک پوشه را هم در حالت No access و هم در حالت Hidden قرار دهیم و بر روی آن پسورد نیز بگذاریم.

درس پنجم:**چگونه پوشه محافظت شده را به حالت عادی برگردانیم؟**

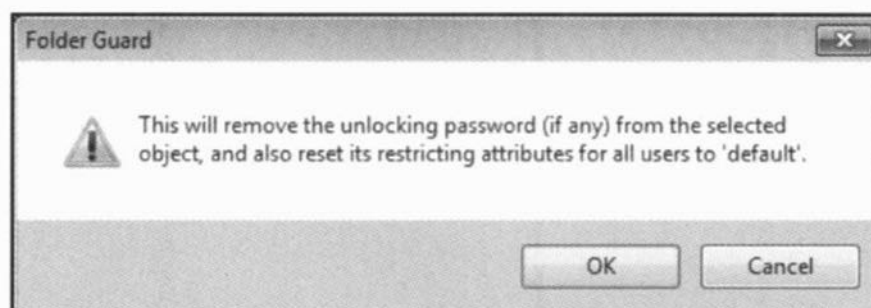
ممکن است بخواهیم پوشه و یا درایوی را که روی آن محدودیت ایجاد کرده ایم و یا روی آن پسورد گذاشته ایم را به حالت عادی و بدون محدودیتی که قبلاً داشته برگردانیم.

برای این کار کافیست به پنجره تنظیمات پوشه یا درایو مورد نظر برویم و سپس روی دکمه Reset attributes کلیک کنیم (تصویر ۱۱۹).



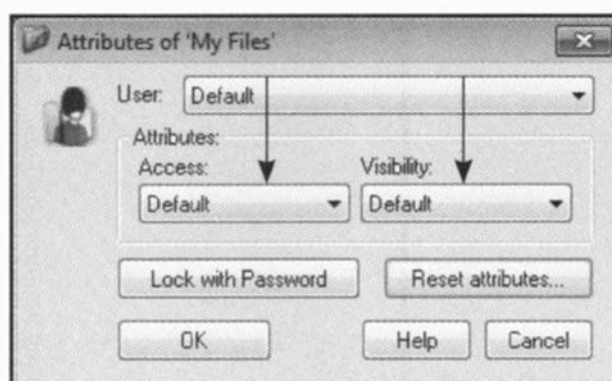
تصویر ۱۱۹

پنجره جدیدی ظاهر می شود که در آن روی دکمه OK کلیک می کنیم
(تصویر ۱۲۰).



تصویر ۱۲۰

با این کار قسمت های Access و Visibility به حالت Default برمی گردند و به همین ترتیب، پسوردی که برای این پوشه قرار داده بودیم، حذف می شود (تصویر ۱۲۱).



تصویر ۱۲۱

سپس روی OK کلیک می کنیم و در پنجره اصلی نرم افزار دکمه
Toggle Protection را روی حالت فعال قرار می دهیم.

فصل سوم

نرم افزار Plain Sight

تا اینجا به روش های مختلفی برای حفاظت از فایل های محرمانه اشاره کردیم. اما علاوه بر این روش ها، روش های دیگری نیز وجود دارند که یکی از آنها پنهان سازی یک فایل در فایل با فرمت دیگر است. برای مثال با استفاده از این روش می توانیم فایل های محرمانه خود را در فایل های تصویری ذخیره کنیم یا اطلاعات خود را در فایل هایی از نوع موسیقی پنهان سازیم. یکی از تفاوت های قابل توجه در استفاده از این روش، شک برانگیز نبودن فایل های مخفی شده است، چرا که این فایل ها دارای فرمت خاصی نیستند و مانند دیگر عکس ها یا موسیقی های ذخیره شده روی هارد دیسک دیده می شوند و فقط ما می دانیم که در قلب آنها اطلاعات دیگری نهفته است!

درس اول: آشنایی با نرم افزار Plain Sight

در این فصل قصد داریم نرم افزاری را پیشنهاد کنیم که این عمل را به بهترین و ساده ترین روش ارائه می کند.

نرم افزار ساده، کم حجم و در عین حال قدرتمند Plain Sight نرم افزاری با روش کار بسیار آسان است که با آن می توانیم به بهترین نحو، اطلاعات محرمانه و ارزشمندمان را از دید کاربران غیرمجاز مخفی نگه داریم. به کمک این نرم افزار می توانیم اطلاعات خود را با هر فرمتی که باشد، در هر فایل با هر فرمتی دیگر پنهان کنیم. همچنین این نرم افزار برخلاف دیگر نرم افزارهای مشابه این امکان را به ما می دهد تا پس از پنهان سازی اطلاعات درون یک فایل، بدون هیچ مشکلی به اجرای فایل اولیه پرداخته و محتویات آن را مشاهده کنیم.

از دیگر قابلیت‌های این نرم‌افزار ایجاد یک فایل کلید برای گشایش فایل‌های مخفی شده است به طوری که حتی وقتی فایل مورد نظر شما که حاوی اطلاعات محرمانه است در اختیار افراد دیگر قرار بگیرد و بتوانند پنهان شدن اطلاعات در این فایل را تشخیص دهند، بدون در اختیار داشتن کلید آن قادر نخواهند بود اطلاعات را بازیابی کنند.

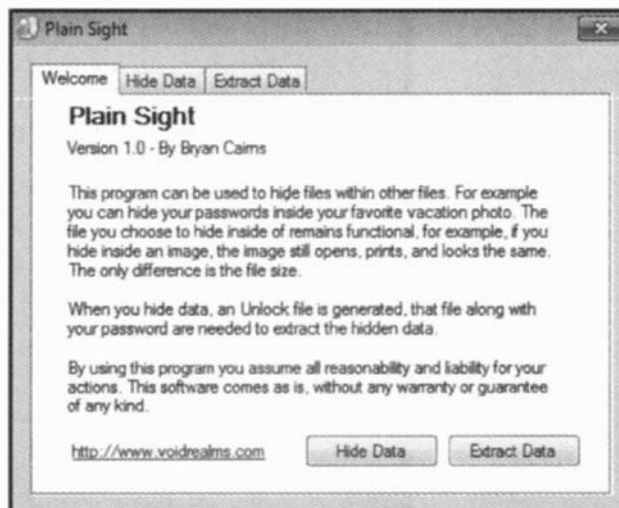
این نرم‌افزار، از یک محکم کاری دیگری نیز برای بالا بردن امنیت استفاده می‌کند. فرض کنیم اطلاعات مورد نظرمان را در یک فایل موسیقی پنهان و کلید آن را در بخشی از هارد دیسک خود ذخیره کرده‌ایم و به خاطر یک بی‌احتیاطی یا آلوده شدن رایانه به ویروس یا نفوذ یک هکر به سیستم، تمام اطلاعات هارد دیسک در اختیار افراد غیرمجاز و البته حرفه‌ای قرار گرفته است. با فرض این که این افراد فایل موسیقی که حاوی اطلاعات محرمانه ماست را پیدا کنند و پس از آن نیز با جستجو میان فایل‌های ما، کلید مورد نظر برای استخراج اطلاعات را نیز پیدا کنند، باز هم نمی‌توانند اطلاعات محرمانه ما را از فایل موسیقی استخراج کنند چرا که این نرم‌افزار برای چنین شرایطی نیز راه حل مطمئنی را در نظر گرفته است و آن راه حل چیزی نیست جز استفاده از یک پسورد برای استخراج فایل‌های مخفی شده!

این نرم‌افزار برای حفاظت هرچه بیشتر از اطلاعات، ما را قادر می‌سازد تا افزون بر پنهان سازی اطلاعات در فایل‌های دیگر و ایجاد کلید برای استخراج آنها، یک پسورد را هم به هر کلید اختصاص دهیم تا در صورت افشا شدن فایل اصلی و کلید آن کسی قادر به بازیابی اطلاعات محرمانه ما نباشد. قابل ذکر است این نرم‌افزار در لوح فشرده همراه کتاب، موجود است.

درس دوم: مخفی سازی اطلاعات در قالب یک فایل دیگر

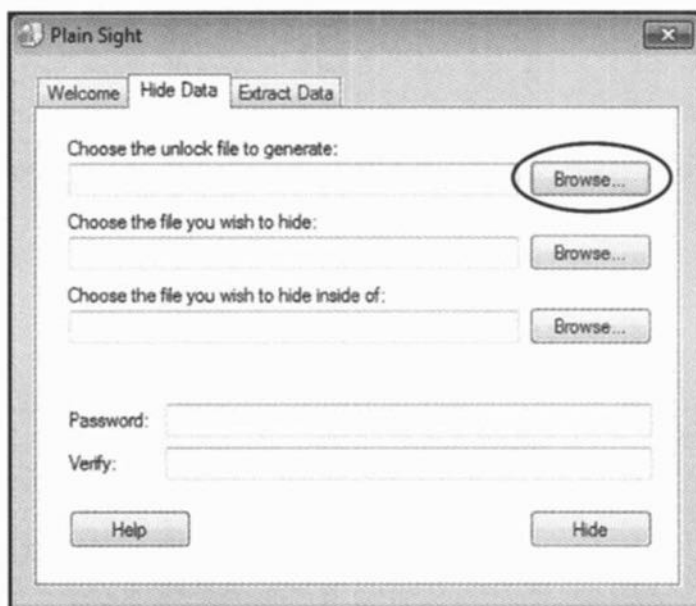
نرم افزار Plain Sight طوری طراحی شده است که می تواند در هر مرحله فقط یک فایل را پنهان کند ولی اگر بخواهیم چندین فایل را در یک فایل مخفی کنیم می توانیم آن فایل ها را در یک پوشه قرار دهیم و سپس آن را با نرم افزاری مثل WinRAR به یک فایل فشرده با پسوند rar تبدیل کنیم. ما در این بخش برای نمونه می خواهیم یک فایل ویدئویی با نام Video.avi را در قالب یک فایل موسیقی با نام Music.mp3 که از قبل در هارد دیسک سیستم ما وجود داشته، پنهان کنیم. هر دوی این فایل ها در دسکتاپ رایانه ما قرار دارند.

روش نصب این نرم افزار بسیار ساده بوده و احتیاجی به کرک ندارد. پس از نصب نرم افزار Plain Sight آن را از روی دسکتاپ اجرا می کنیم (تصویر ۱۲۲).



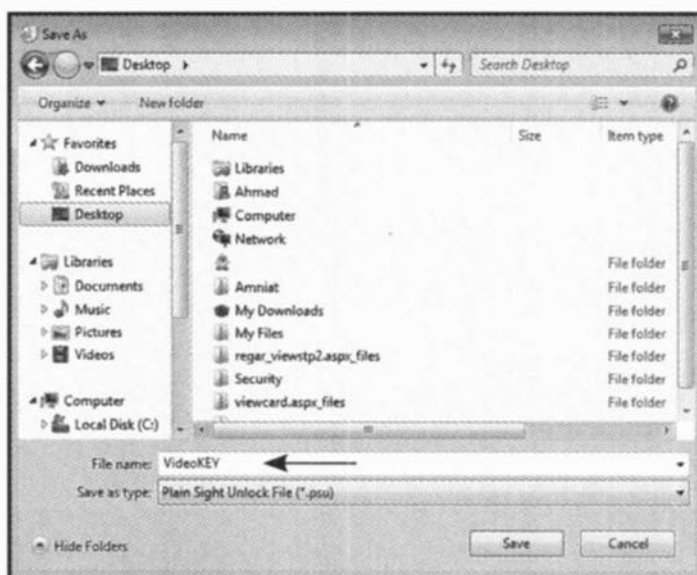
تصویر ۱۲۲

به سربرگ Hide Data می رویم. ابتدا باید یک فایل کلید برای استخراج فایل مخفی شده ایجاد کنیم. در قسمت Choose the unlock file to generate روی دکمه Browse کلیک می کنیم (تصویر ۱۲۳).



تصویر ۱۲۳

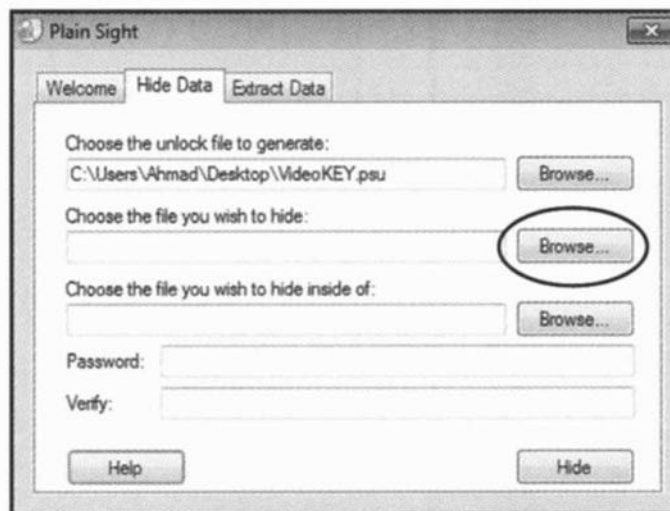
پنجره‌ای باز می‌شود که در آن مکان ذخیره شدن فایل کلید و نام آن را تعیین می‌کنیم. ما نام این کلید را VideoKEY گذاشته و آن را با کلیک روی دکمه Save در دسکتاپ ذخیره می‌کنیم (تصویر ۱۲۴).



تصویر ۱۲۴

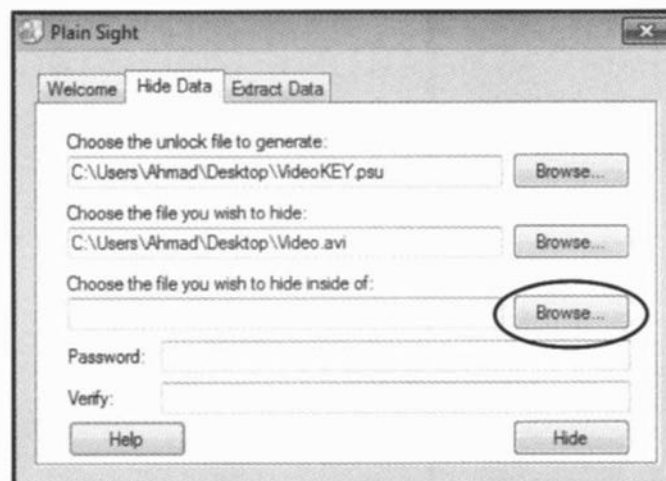
با این کار یک فایل با نام VideoKEY.psu در دسکتاپ ایجاد خواهد شد.

در مرحله بعد فایل‌هایی که می‌خواهیم مخفی کنیم را باید انتخاب کنیم. برای این کار در قسمت Choose the file you wish to hide روی دکمه Browse کلیک می‌کنیم (تصویر ۱۲۵).



تصویر ۱۲۵

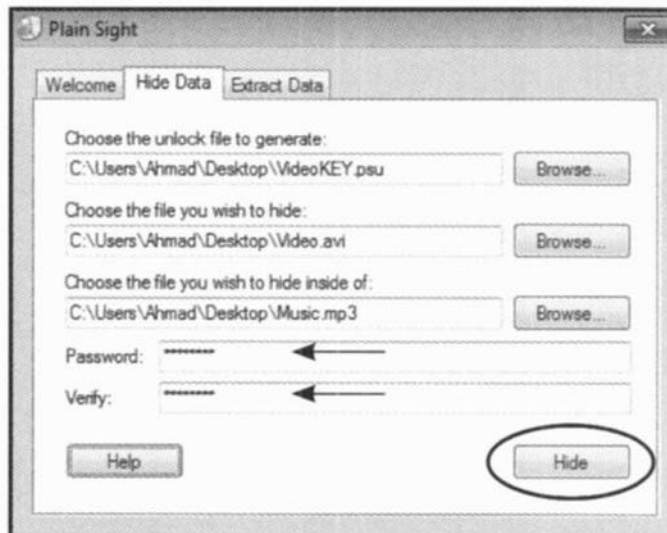
در پنجره باز شده فایل ویدئویی Video.avi را انتخاب می‌کنیم و سپس روی Open کلیک می‌کنیم. در مرحله بعد فایل‌هایی که می‌خواهیم ویدئوی مورد نظر ما در آن مخفی شود را باید انتخاب کنیم. برای این کار در قسمت Choose the file you wish to hide inside of روی دکمه Browse کلیک می‌کنیم (تصویر ۱۲۶).



تصویر ۱۲۶

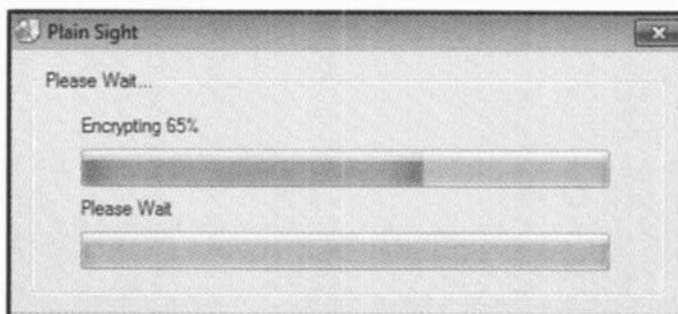
در پنجره بازشده فایل موسیقی Music.mp3 را انتخاب کرده و سپس روی دکمه Open کلیک می‌کنیم.

تابه اینجا فایل‌های کلید، مخفی شونده و مخفی کننده را تعیین کرده‌ایم. حالا برای این که امنیت را بالا ببریم باید پسوردی را برای استخراج فایل مخفی شده در نظر بگیریم. برای این کار در قسمت Password پسورد دلخواه‌مان را وارد کرده و در قسمت Verify آن را دوباره تکرار می‌کنیم (تصویر ۱۲۷).



تصویر ۱۲۷

حالا فقط کافیست روی دکمه Hide کلیک کنیم و منتظر بمانیم تا عملیات پنهان سازی به پایان برسد (تصویر ۱۲۸).



تصویر ۱۲۸



تصویر ۱۲۹

بعد از اتمام کار پنجره کوچکی با پیام "Done" ظاهر می‌شود که در آن باید روی دکمه OK کلیک کنیم (تصویر ۱۲۹).

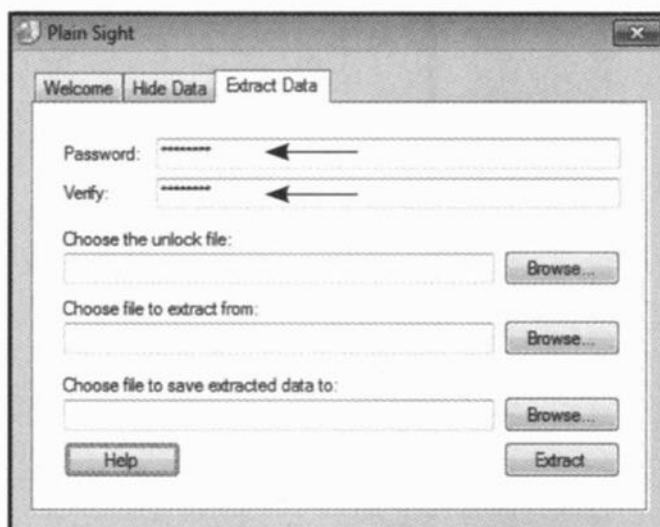
حالا ما یک فایل موسیقی با نام Music.mp3 داریم که در قلب آن یک فایل ویدئویی مخفی شده است.

این فایل موسیقی بدون هیچ مشکلی اجرا می‌شود. تنها تغییری که در این فایل به وجود آمده، حجم آن است که به اندازه حجم فایل ویدئویی به آن اضافه شده است. در درس بعد آموزش خواهیم داد که چطور این فایل ویدئویی مخفی شده را بازیابی یا استخراج کنیم.

درس سوم: بازیابی فایل مخفی شده

برای بازیابی فایل ویدئویی که در بخش قبل آن را مخفی کرده بودیم مراحل زیر را انجام می‌دهیم:

ابتدا در نرم‌افزار Plain Sight به سربرگ Extract Data می‌رویم. پسورد رادر قسمت‌های Password و Verify وارد می‌کنیم (تصویر ۱۳۰).



تصویر ۱۳۰

در مرحله بعد باید فایل کلیدی که در بخش قبلی با نام VideoKEY.psu ایجاد کرده بودیم را انتخاب کنیم. برای این کار در قسمت Choose the unlock file با کلیک روی دکمه Browse فایل کلید را که در دسکتاپ قرار داده‌ایم انتخاب می‌کنیم (تصویر ۱۳۱).



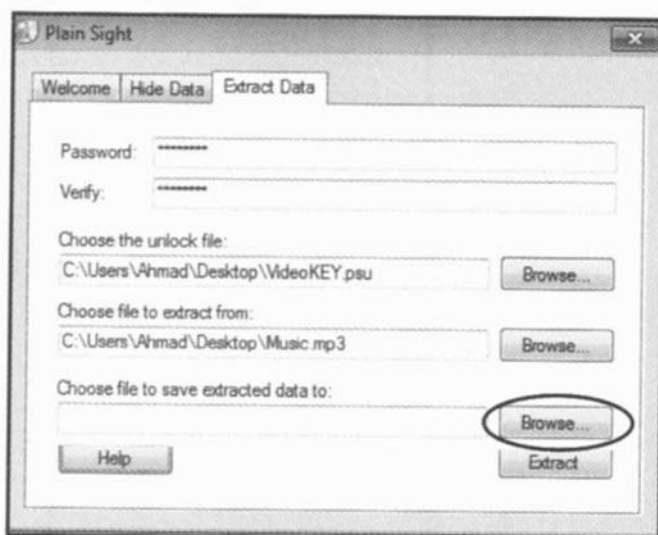
تصویر ۱۳۱

در مرحله بعد در قسمت Choose file to extract from با کلیک روی دکمه Browse فایل موسیقی که حاوی فایل ویدئویی مخفی شده ما می‌باشد را انتخاب می‌کنیم (تصویر ۱۳۲).



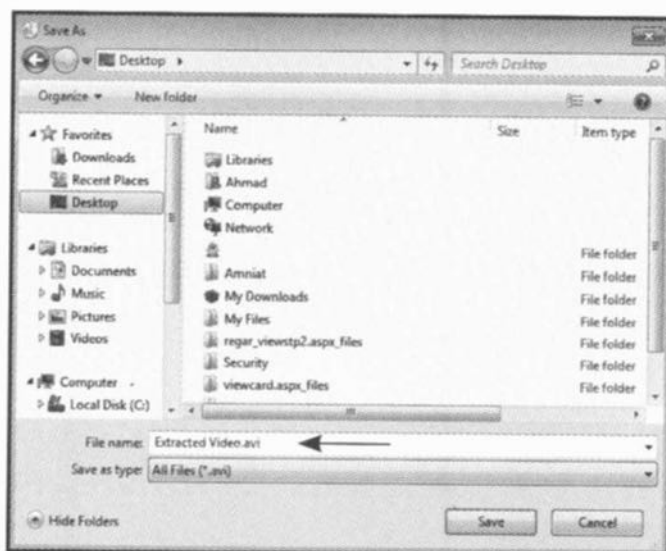
تصویر ۱۳۲

در مرحله بعد با کلیک روی دکمه Browse در قسمت Choose file to save extracted data to نام و مکان ذخیره شدن فایل ویدئویی را انتخاب می‌کنیم (تصویر ۱۳۳).



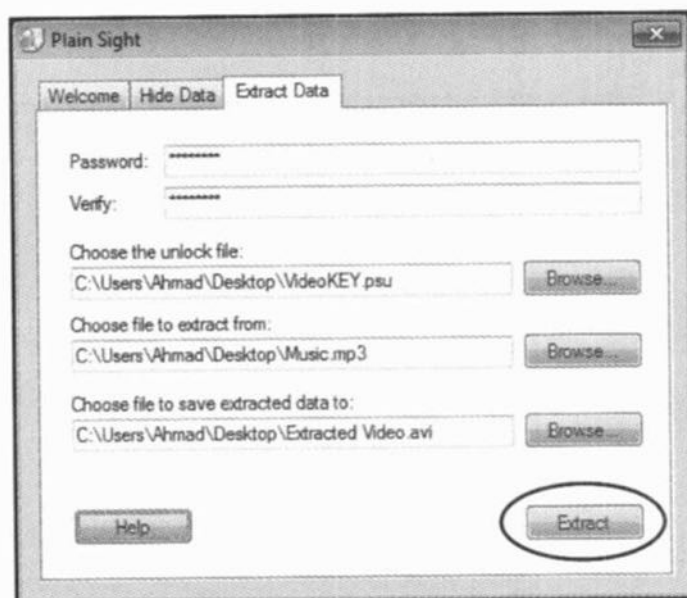
تصویر ۱۳۳

ما نام آن را Extracted Video.avi گذاشته و آن را در دسکتاپ ذخیره می‌کنیم. سپس روی Save کلیک می‌کنیم (تصویر ۱۳۴).



تصویر ۱۳۴

تنها کاری که باقی مانده این است که روی دکمه Extract کلیک کنیم و تا پایان یافتن عمل بازیابی صبر کنیم (تصویر ۱۳۵).



تصویر ۱۳۵

با ظاهر شدن پیغام "Done" روی دکمه OK کلیک می‌کنیم. فایل ویدئویی Video.avi که قبلاً آن را مخفی کرده بودیم حالا با نام Extracted Video.avi در دسکتاپ ما جای گرفته است.

نکته ...

هر کاربری که این سه مورد یعنی فایل و پسورد مورد نظر و فایل کلید آن را داشته باشد می‌تواند فایل مخفی شده را با نرم‌افزار Plain Sight استخراج کند و به آن دسترسی داشته باشد. به عنوان مثال می‌توانیم این سه مورد را با ایمیل برای شخصی دیگر بفرستیم و آن شخص با داشتن این اطلاعات، فایل مخفی شده را در رایانه خودش استخراج و از آن استفاده کند.

فصل چهارم

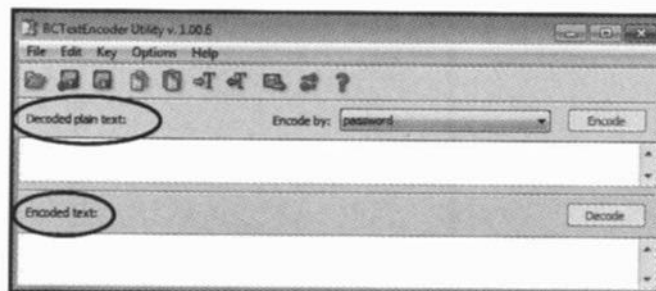
نرم افزار BC Text Encoder

درس اول: آشنایی با نرم افزار BC Text Encoder

نرم افزار BC Text Encoder نرم افزاری کوچک و رایگان می باشد که به وسیله آن قادریم متن ها و نوشته های فارسی و یا انگلیسی را رمز نگاری کنیم تا دیگران توانایی خواندن آن را نداشته باشند و فقط با داشتن پسورد بتوانیم متن را رمزگشایی نماییم. لازم به ذکر است که این نرم افزار فقط از فایل های با پسوند txt پشتیبانی می کند. پس اگر متن مورد نظر ما فرمت دیگری دارد کافیه متن را در نرم افزاری مثل Notepad کپی کرده و سپس آن را با پسوند txt ذخیره کنیم. (این نرم افزار در لوح فشرده همراه کتاب موجود می باشد) نرم افزار BC Text Encoder نیازی به نصب ندارد و برای اجرای آن کافیه فقط روی فایل BCTextEncoder.exe جفت کلیک کنیم.

صفحه اصلی این نرم افزار از دو بخش اصلی Decoded plain text و Encoded text تشکیل شده است.

در قسمت Decoded plain text می توانیم متن خود را بنویسیم و یا این که یک فایل متنی را اضافه کنیم. در قسمت Encoded text متن رمزنگاری شده به نمایش در می آید (تصویر ۱۳۶).

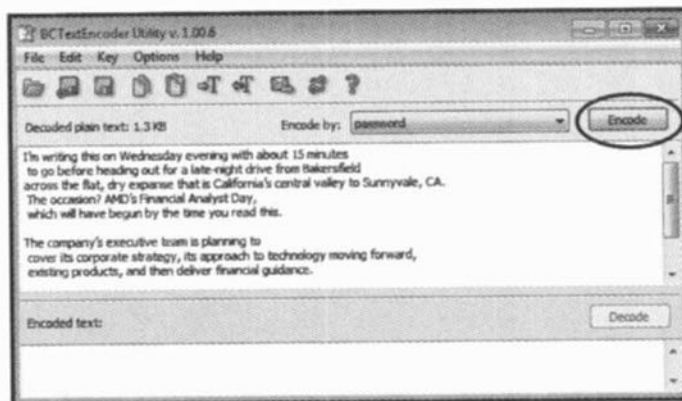


تصویر ۱۳۶

درس دوم: رمزنگاری یک متن

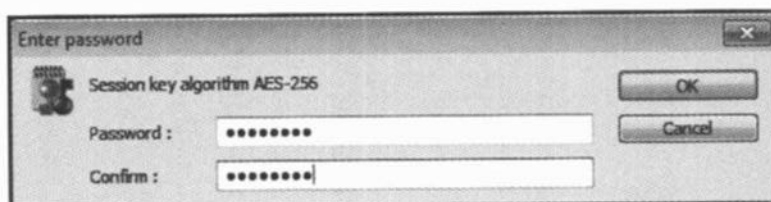
در این بخش می‌خواهیم یک فایل متنی با نام My Text.txt را رمزنگاری کنیم. برای این کار ابتدا نرم‌افزار را اجرا می‌کنیم. از منوی File گزینه Open را انتخاب می‌کنیم.

سپس فایل My Text.txt که در دسکتاپ گذاشته‌ایم را انتخاب می‌کنیم. با این کار متن این فایل در قسمت Decoded plain text نمایش داده می‌شود. روی دکمه Encode کلیک می‌کنیم (تصویر ۱۳۷).



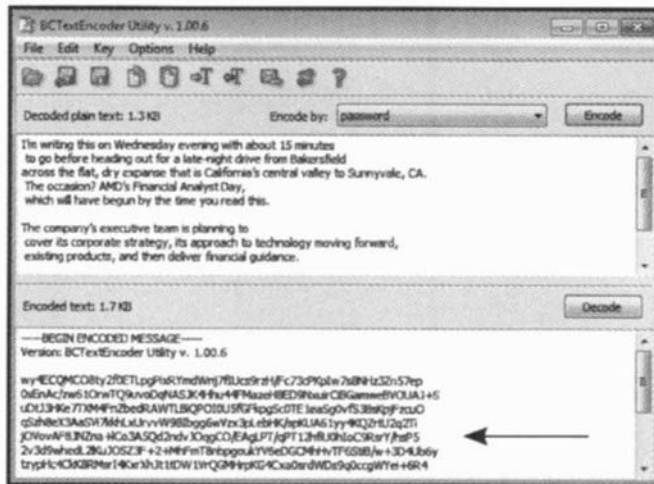
تصویر ۱۳۷

پنجره‌ای باز می‌شود که در آن پسوردی را به طور یکسان در هر دو کادر وارد می‌کنیم (تصویر ۱۳۸).



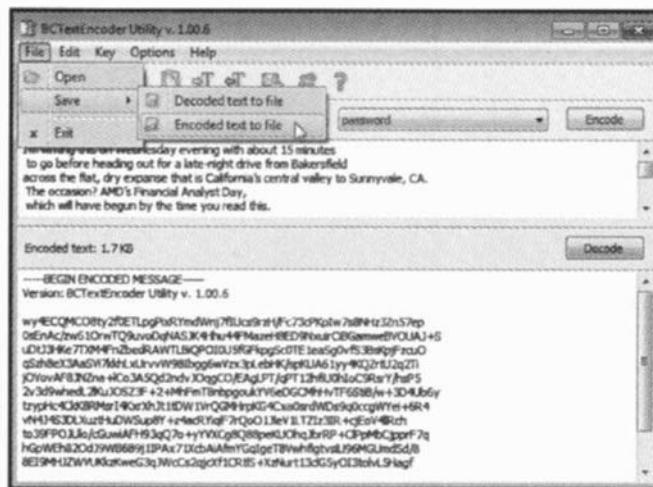
تصویر ۱۳۸

با کلیک روی OK متن ما رمزنگاری می‌شود. این متن که به صورت رمز در آمده در قسمت Encoded text نمایش داده می‌شود (تصویر ۱۳۹).



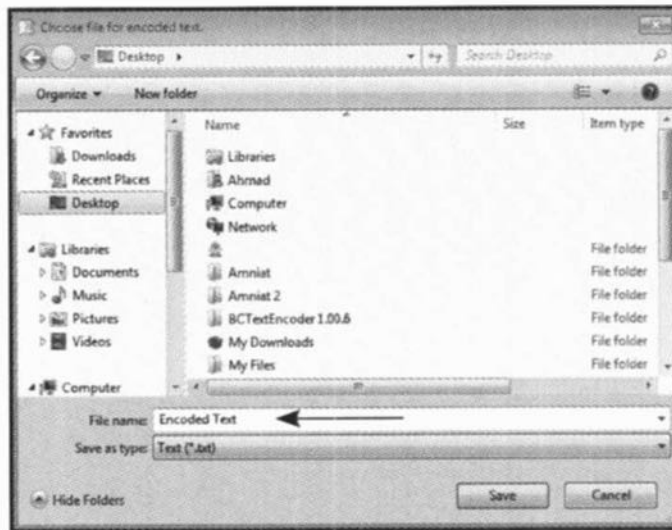
تصویر ۱۳۹

حال برای ذخیره این متن رمزی، از منوی File گزینه Save را انتخاب کرده و از منوی باز شده گزینه Encoded text to file را انتخاب می‌کنیم (تصویر ۱۴۰).



تصویر ۱۴۰

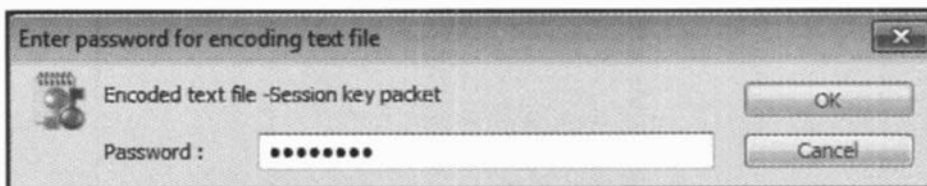
در پنجره باز شده در قسمت File Name نام Encoded Text را برای این فایل رمزی وارد کرده و سپس با کلیک روی دکمه Save آن را در دستکاپ ذخیره می‌کنیم (تصویر ۱۴۱).



تصویر ۱۴۱

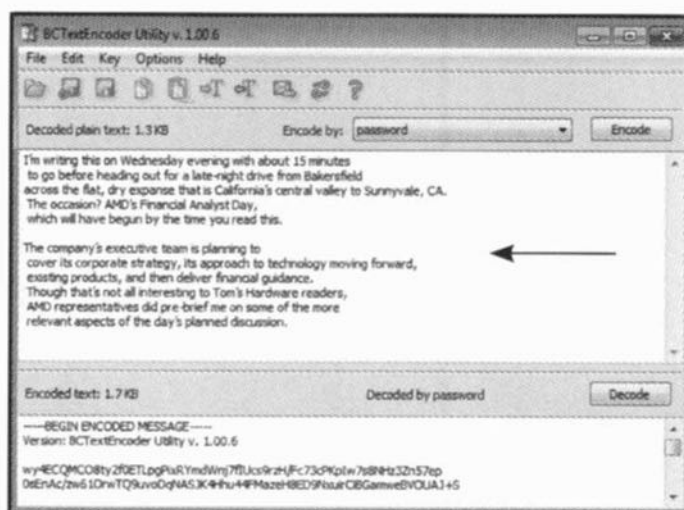
درس سوم: رمز گشایی یک متن رمزنگاری شده

در این بخش می‌خواهیم فایل متنی که در بخش قبلی ایجاد کرده بودیم را رمزگشایی کنیم. برای این کار در صفحه اصلی نرم‌افزار از منوی File گزینه Open را انتخاب می‌کنیم. در پنجره باز شده فایل Encoded Text.txt را انتخاب می‌کنیم. با این کار پنجره جدیدی باز می‌شود که پسورد را در آن وارد کرده و سپس روی دکمه OK کلیک می‌کنیم (تصویر ۱۴۲).



تصویر ۱۴۲

متن مورد نظر ما رمزگشایی شده و در قسمت Decoded plain text نمایش داده می‌شود (تصویر ۱۴۳).



تصویر ۱۴۳

متن رمزگشایی شده را می‌توانیم از مسیر **File→Save→Decoded text to file** ذخیره نماییم.

سخن آخر

امیدواریم که مطالب موجود در این کتاب، نظر شما را جلب کرده باشد و شما مطالب مد نظرتان را در آن یافته باشید. به هر حال سعی ما بر این بود که با بیانی ساده و روش‌های آسان، کارکرد نرم‌افزارهای امنیت اطلاعات را خدمتان آموزش دهیم. همانطور که در پیشگفتار هم عرض کرده بودیم، نرم‌افزارهای زیادی در حوزه امنیت اطلاعات وجود دارند. اکنون که شما دوستان عزیز با مفاهیم امنیت، نرم‌افزارهای امنیتی و... آشنا شدید، می‌توانید با یک جستجوی ساده در محیط اینترنت به راحتی به انواع مختلفی از این نرم‌افزارها دسترسی پیدا کنید و کار کردن با آنها را نیز امتحان کنید.

در پایان از پدر و مادرمان که با محبت و دلسوزی‌شان، راه‌های پیشرفت را برایمان نمایان می‌کنند تشکر و قدردانی می‌کنیم و بوسه بر دستانشان می‌زنیم.

از این مجموعه منتشر شده است

کلید نرم افزارهای گوگل

معمولاً گوگل را با موتور جستجوی قوی آن می‌شناسند. اما شرکت گوگل نرم افزارهای کاربردی زیادی را نیز به دنیای اینترنت معرفی کرده است که در این کتاب روش کار با تعدادی از آن‌ها را خواهید آموخت.

یکی از نرم افزارهای آموزش داده شده در این کتاب Google Desktop است که با آن می‌توانید اطلاعات مورد نیاز از درون کامپیوترتان را بیابید. مثلاً اگر یک فایل Word را در کامپیوتر گم کرده باشید، نامش را هم فراموش کرده باشید ولی بدانید که متنش در چه موردی بوده چطور آن را پیدا می‌کنید؟ این یکی از قابلیت‌های خوب Google Desktop است

با مطالعه این کتاب، مجموعه‌ای از نرم افزارهای گوگل را می‌شناسید که

زندگی را برای شما آسان‌تر و زیباتر می‌کند.



کلید بازیابی اطلاعات (ویراست دوم)

مطالعه این کتاب از اهمیت زیادی برخوردار است. تقریباً همه کسانی که با رایانه کار می‌کنند به نوعی در معرض خطر از دست رفتن اطلاعات هستند و باید با مباحث بازیابی اطلاعات آشنا باشند چه شخصی که تازه با دنیای رایانه آشنا شده و چه کسی که سال‌ها است که با آن کار می‌کند. در دنیای رایانه که بخش اعظم کار با آن ذخیره سازی اطلاعات و اسناد و سپس بایگانی آنهاست، دو بخش فوق‌العاده حساس پشتیبان‌گیری (Backup) و بازیابی (Recovery) از امور اجتناب ناپذیر کار است. با مطالعه این کتاب از بسیاری از مشکلات احتمالی جلوگیری می‌کنید، چیزی است شبیه به واکسن زدن برای پیشگیری از ابتلا به بیماری.



کلید ساخت بازی

ویژگی اکثر افراد این‌طور است که اگر کالا یا هر چیزی را با دست خود ایجاد کنند برایشان جذابیت و حس زیباتری دارد هر چند اگر مشابه آن کالا در بازار با امکانات بیشتر هم موجود باشد. مقوله‌ی بازی سازی نیز همین‌طور است. یعنی به کمک یک نرم افزار می‌توانیم به راحتی بازی‌هایی را با فکر و ایده‌ی خودمان ایجاد کنیم. بنابراین کسانی که به ساخت بازی علاقه‌مند هستند می‌توانند از این کتاب استفاده‌ی لازم را ببرند. در ضمن باید متذکر شویم که خواننده‌ی این کتاب لازم نیست پیش‌زمینه‌ای در مورد بازی سازی داشته باشد.

