بسم الله الرحمن الرحيم

اخر تحديث بتاريخ

1/1/2015

شرح احسبة كامل حول امن المعلومات وتشفير الاتصالات والتعامل مع الصور والاجهزة الذكية وكشف التلغيم وتحليل العمليات والحماية من الاختراق وتتبع عنوان المخترق لتحديد مكانة

بعد الحملة الشرسة ضد من يكتب وينقل حقيقة مايحدث في الارض واغلاق الحسابات المتكرر على تويتر لا شك ان امن اتصالك مهم ولهذا قمت باعداد هذا الشرح القديم المجدد بشكل مفصل ويشمل الشرح تشفير الاتصال . تشفير الجهاز كامل اجزء من الهارديسك او) ملف معين . تشفير اتصال الهاتف الجوال. خدمة البريد الاكتروني المشفر الامن . تغير المواقع الجغرافية لصورك . برامج المحادثة المشفرة . تجميد نظام التشغيل . التعامل في البيئة الوهمية.تنصيب نظام وهمي داخل النظام الاساسي . برامج حماية وجدار ناري . تحليل الملفات لكشف تلغيمها . الكشف على اتصالات شبكة جهازك ومعرفة الاختراق عن طريق الـ DNS . وساقوم باضافة بعض النقاط بتعديل على (تحليل برامج الجهاز بستخدام هيجاك نفس هذه الصفحة في وقت لاحق ان شاء الله لزيادة المعلومات

اعداد : عمروف الجلاد

JladOmarov@

ask.fm

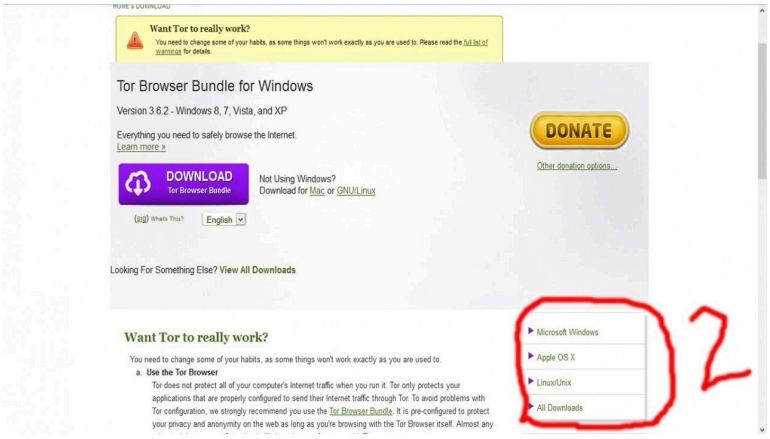
تتشفير اتصالك واستخدام شبكات التور و الفي بي ان

لمن يستخدم نضام ويندوز او ماك او لينكس

انصحك بشبكة التور وهي تعتبر اكثر الشبكات امن

https://www.torproject.org/index.html.en

بعد الدخول على الرابط تابع الصور



بعد اختيار نظام التشغيل الخاص بك حمل ونصب البرنامج ستظهر لك هذه الايقونة على سطح المكتب انقر علية لتشغلها وسيفتح معك متصفح خاص بالشبكة

عند فتح البرنامج سيتم الاتصال خلال ثواني بسرافرات شبكة التور وسيفتح متصفح فايرفوكس خاص بشكبة تور يقوم بمسح كل مخلفات التصفح

بعد ان يفتح هذه المتصفح انت في امان تام ان شاء الله قول ما احببت

اصحاب الايفون والايباد و الجالكسي

لا يوجد برنامج تور للايفون او الايباد الا بلجلبيرك (كسر قيد الجهاز) لكن هناك بديلان الاول بمقابل مالي والثاني مجاني و سا اشرح الطريقتين

ملاحظة: يوجد برنامج تور لجميع اجهزة اندرويد

الطريقة الاولى

الدخول على هذا الروابط وتحميل برنامج

SecureLine VPN

وهو مجاني لمدة اسبوع واحد

رابط البرنامج من ابل ستور

https://itunes.apple.com/us/app/secureline-vpn-wifi-security/id793096595?mt=8

رابط البرنامج من غوغل بلاي

https://play.google.com/store/apps/details?id=com.avast.android.vpn&hl=cs

بعد التحميل شغل البرنامج وفعل الفي بي ان في اعدادت الجهاز البرنامج يشرح طريقة التشغيل عند بداية العمل بعد ظهور شعار الفي بي ان في جهازك تكون جميع معلوماتك مشفرة ويستحيل تتبعك

برنامج اخر عالي التشفير

ايفون

Freedome

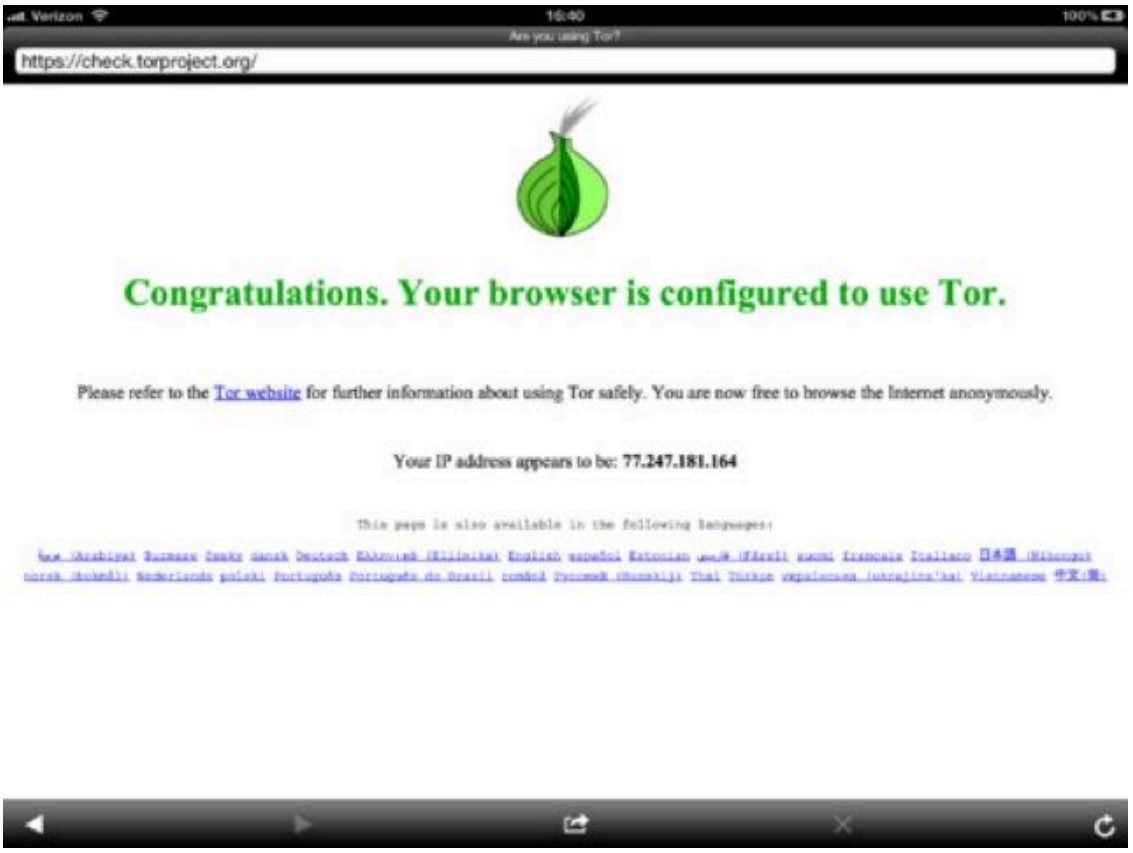
اندرويد

freedome.vpn

*المتصفحات الامنة والمشفرة للايفون و اندرويد

يعتمد على شبكة التور المشفرة وتحميك بعد الله من الملاحقة الامنية وتحديد موقعك

متصفح onionbrowser



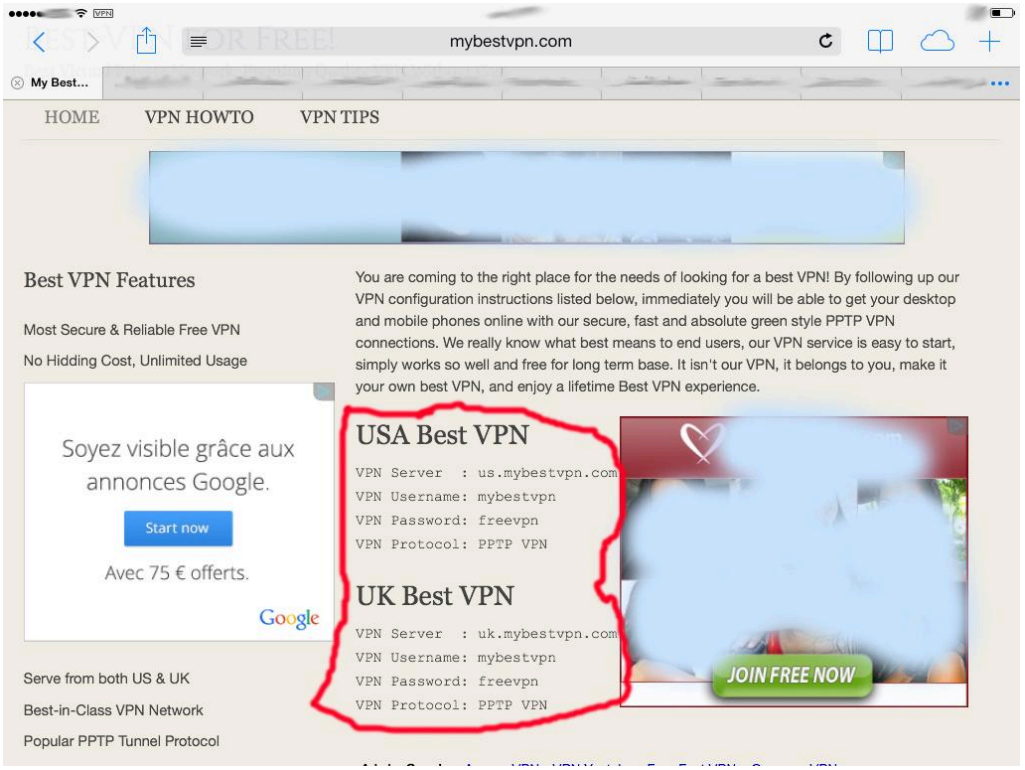
للتحميل من ابل ستور الخاص بالآيفون هنا

طريقة ثانية للايفون والايباد وهي مجانية (غير امنه) تابع معي بالصور

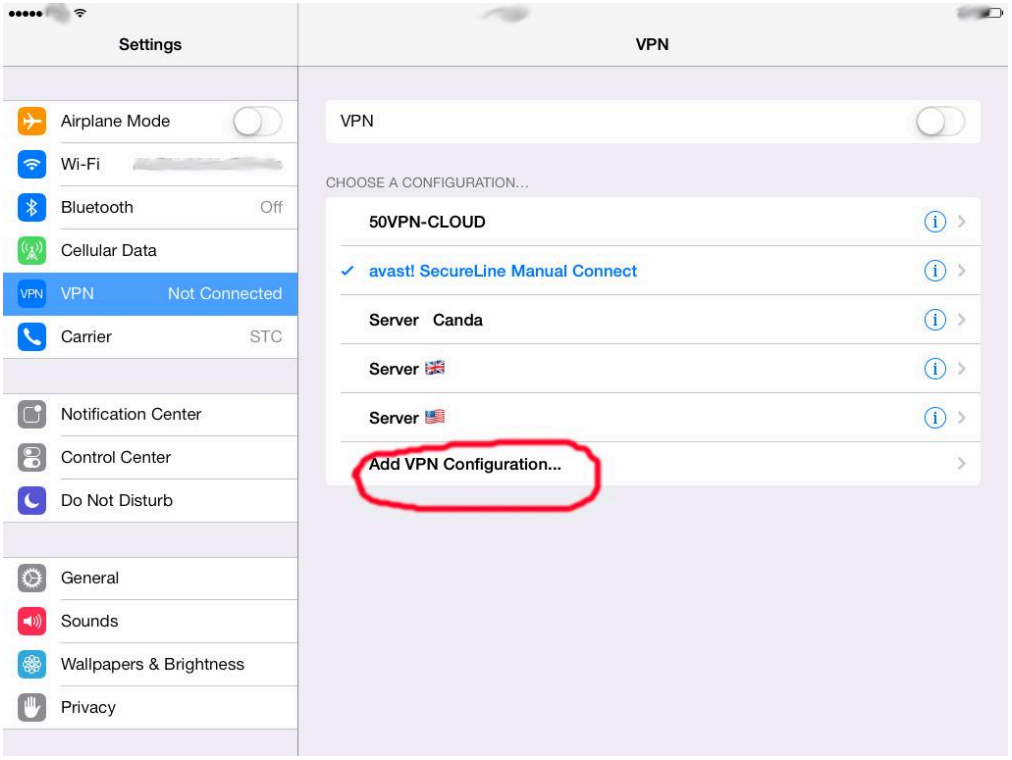
ادخل على هذا الرابط مع العلم انه محجوب لكن ساضع لكم بيانات شبكة في بي ان في اخر الموضوع

ادخل على هذا الرابط

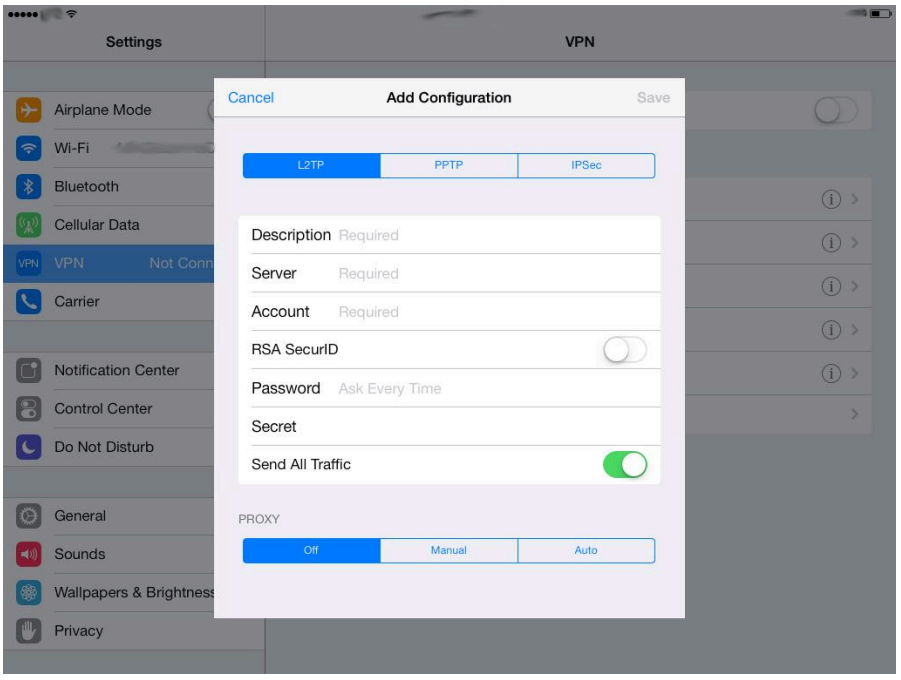
http://mybestvpn.com/



اختر احد السيرفرات وخذ البينات ثم نروح لعدادت الايفون او الايباد



الان نضع البيانات الي اخذناها حسب برتكول الشبكة ونشغل الفي بي ان



بيانات سيرفر في بي ان

VPN

USA Best VPN

VPN Server : us.mybestvpn.com
VPN Username: mybestvpn
VPN Password: freevpn
VPN Protocol: PPTP VPN

UK Best VPN

VPN Server : uk.mybestvpn.com
VPN Username: mybestvpn
VPN Password: freevpn
VPN Protocol: PPTP VPN

---

* امن الصور

جميع الصور الملتقطة بهواتف ذكية او كميرات حديثة تقوم بحفظ الموقع الجغرافي لكل صورة ملتقطة او تصوير للشاشة الجهاز والحل بتغير الموقع الجغرافي للصورة بحيث تظهر عند تحليلها من اجهزة الامن انها ملتقطة في اي بلد انت تختاره وانصح بستخدام برنامج

Photo GPS Editor

لسهولة استخدامة

---

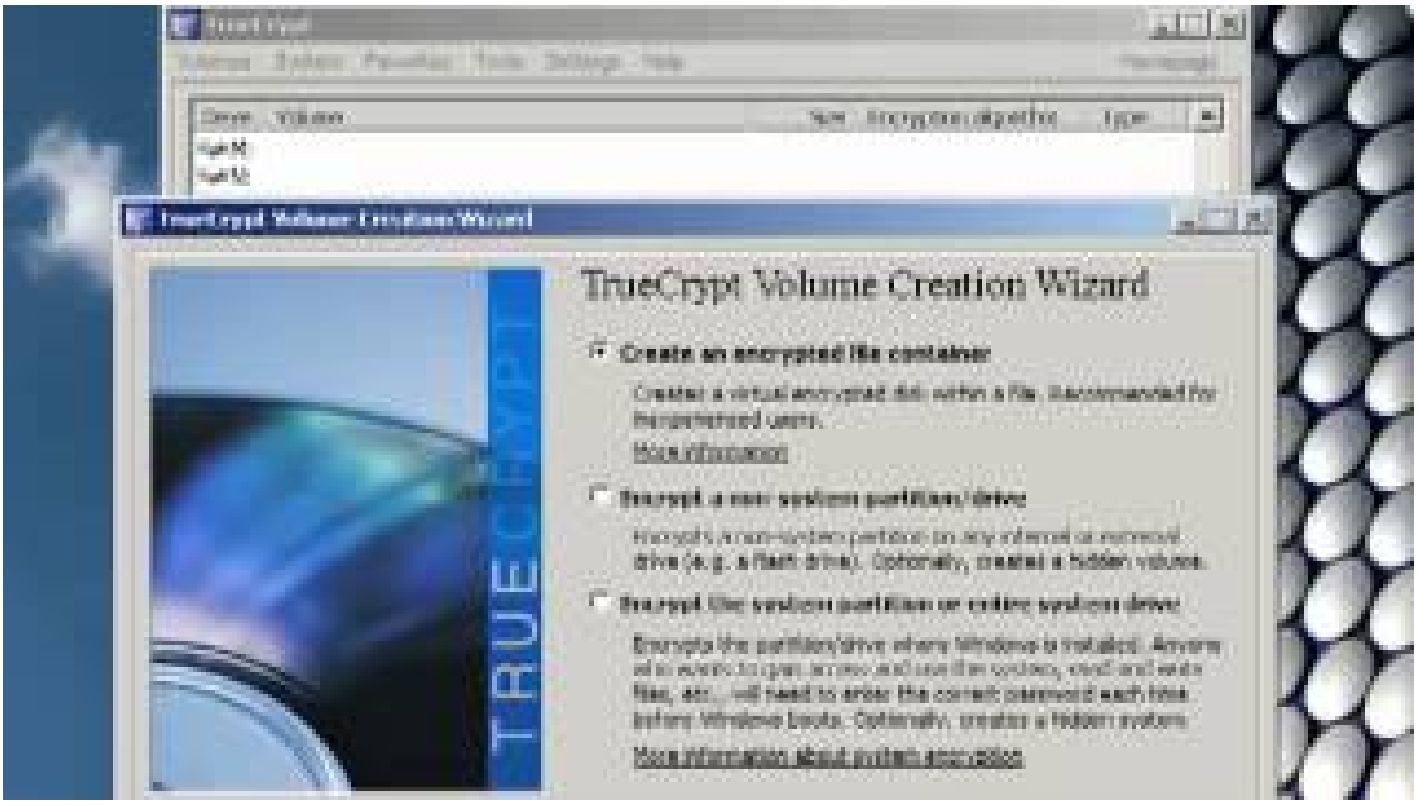
* تشفير الأجهزة بالكامل او جزء من الهارديسك

لتشفير جهازك بالكامل او جزء من الهارديسك او ملف معين مهما كان انصحك بستخدام هذا البرنامج

True Crypt لتحميل اضغط على هنا

TrueCrypt

شرح البرنامج فديو



الهارد ديسك المشفر ذاتي يقوم بتشفير كافة البيانات ولايمكن فتح الهارديسك الا برقم سري
مشفر وهو الاخر مصمم لتقديم الحماية القصوى
انصح الجميع بقتناءة وهو موجود على متجر امازون او في المحلات الكبرى

---

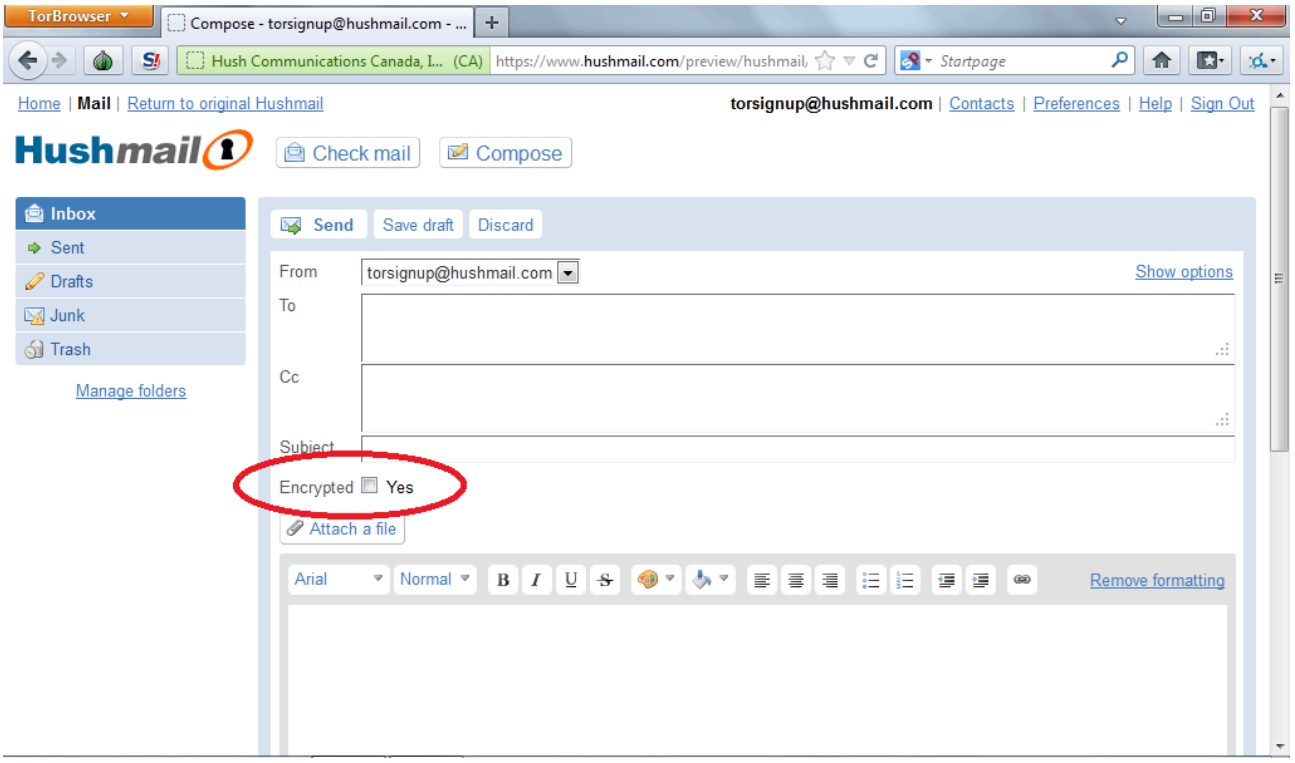
*البريد الاكتروني المشفر بالكامل

Tutanota®
einfach. sicher. mailen.

لتسجيل في الخدمة من هنا

خدمة كندية عالية التشفير

Hushmail .com



البريد المرسل مشفر بدون الكبس على زر التشفير اما اذا كبست على هذا الزر المشار الية ستكون اضفت تشفير برقم سري زيادة على التشفير العادي ولن يستطيع احد الاطلاع على الرسالة الا بهذا الرقم السري الذي انشئته لاغلاق الرسالة بعد تشفيرها وارسالها لكن يجب ان يكون المرسل الية يعرف الرقم السري لكي يستطيع فتح الرسالة

[للتسجيل في الخدمة من هنا]

---

* التراسل الامن عبر برامج الاجهزة الذكية

لاشك ان الجميع يستخدم برنامج وات ساب لكن هذا البرنامج غير مشفر وغير امن مزود الخدمة لديك يستطيع التجسس علية والهكر ايظن عن طريق التنصت على الشبكة وحين تكتب رسالة تظهر من غير تشفير للهكر

البديل هو برنامج **Telegram الذي يحتوي على خدمة التحادث المشفر الامن**

تحميل البرنامج للايفون من هنا

تحميل البرنامج اندرويد من هنا

برنامج Threema

برنامج ثريما مشفر بالكامل صور وفديو ومحادثات صوتية ولا يعتمد على رقم الهاتف بل على اسم مستخدم (يوزر) وهو امن للمحادثات ولا يمكن التجسس علية

لتحميل البرنامج للايفون من هنا

لتحميل البرنامج للاندرويد من هنا

---

* برامج الحماية

لتئمين جهازك من احصنة طروادة التروجان او الباتش او الباك دور عليك اول ببرامج الحماية والجدار الناري

انصح بالدب الروسي برنامج

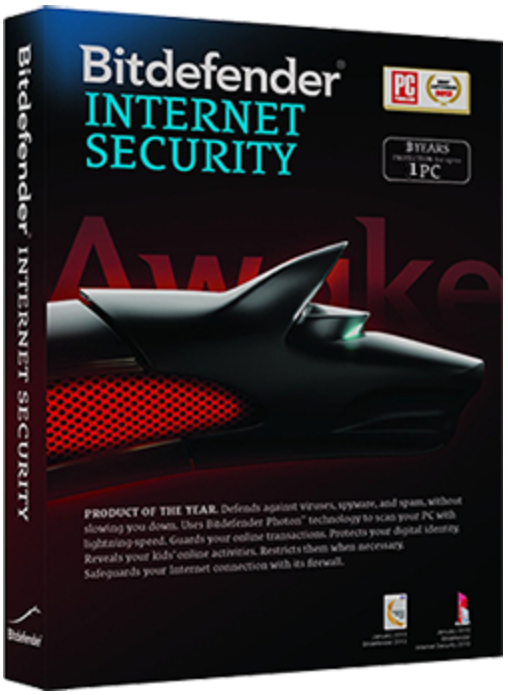
kaspersky internet security 2015

لشراء البرنامج من هنا

برنامج خارق يقدم الحماية القصوى

العملاق الروماني برنامج

bitdefender



لتحميل البرنامج من هنا لنسخة 64 بيت او من هنا لنسخة 32 بيت

مفاتيح التفعيل

3A64FDB6947804D42CD4

9CFE119A7A6831B18B00

6HAX5LK

32EE6B1B7B5CD47DCDA7

718F8E40CA837A40A14B

GAB55GV

C2C3CC22BD78378B6C65

RG7CBKG

62188B528CD2A1BBCD0B

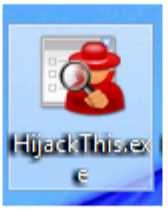
PMDNC2Q

EFEE007DFE525F30D185

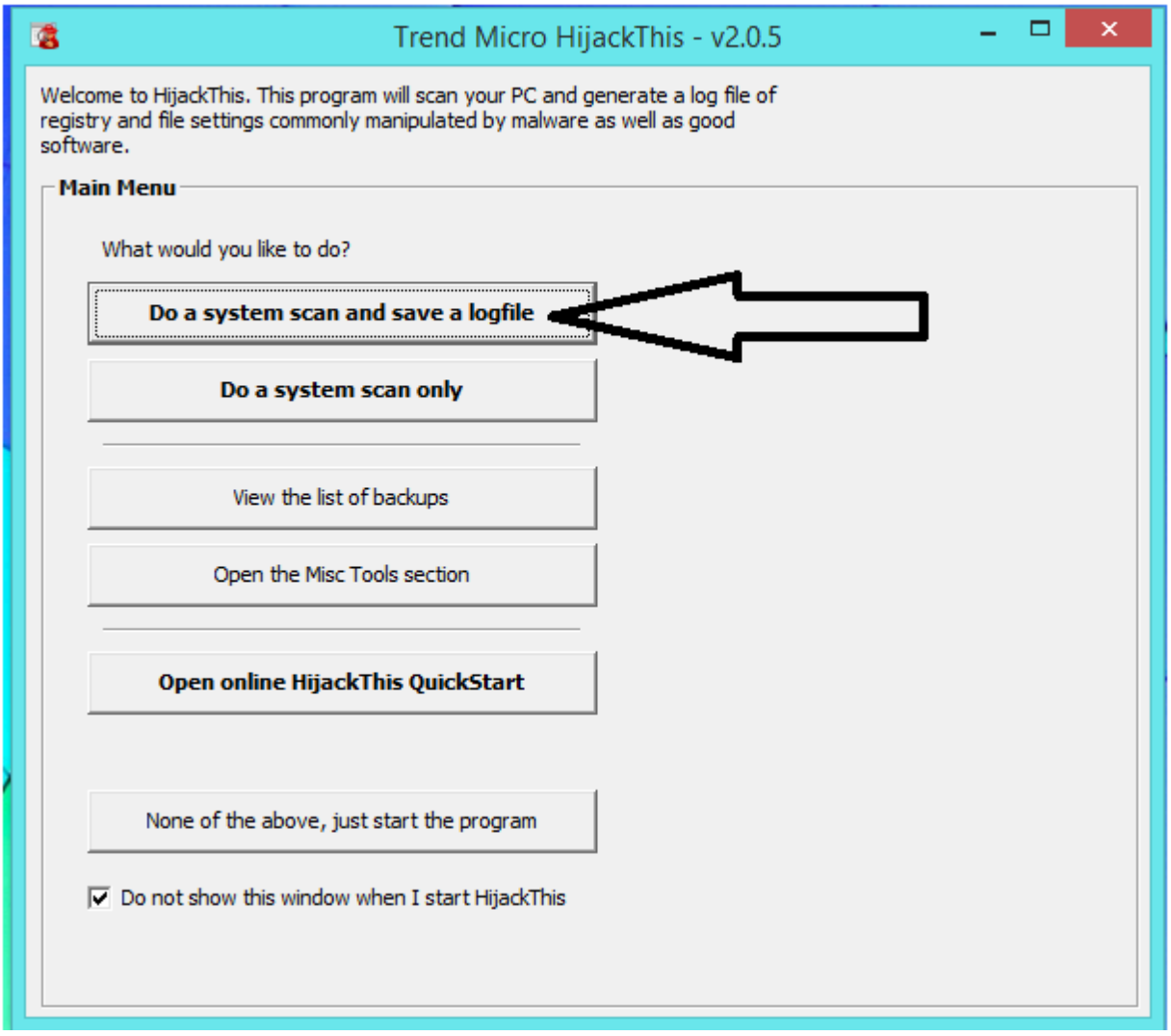
تنتهي في تاريخ 26 \7 \2017

***تحليل الملفات وكشف التلغيم**

ورابط التحميل في HijackThis تحليل البرامج التي تعمل على الجهاز بستخدام اداة الاسفل



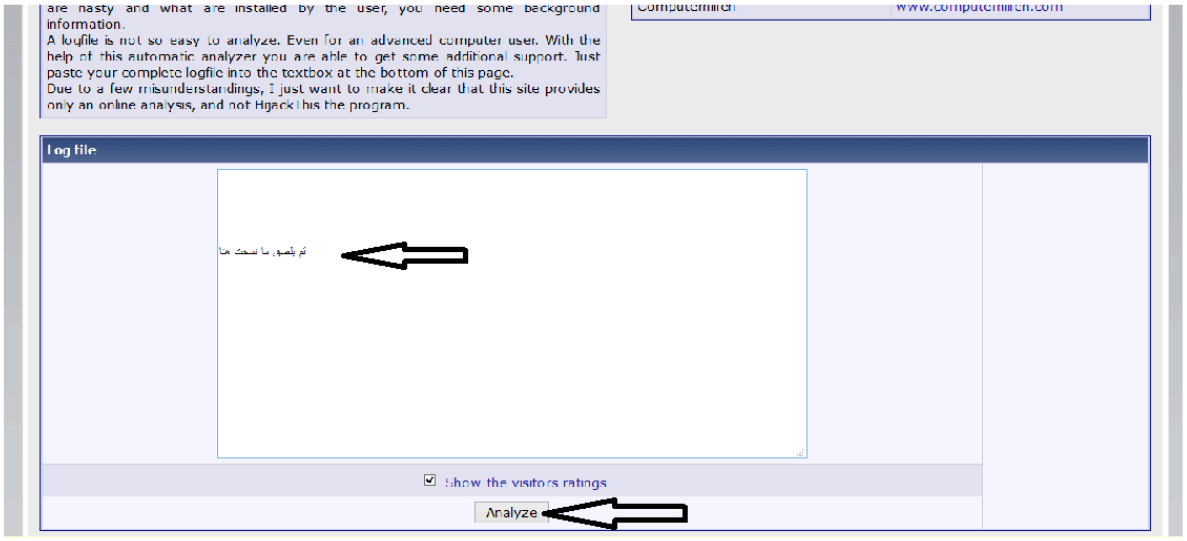
شغل الاداة كمسؤول ثم وافق على الاتفاقية



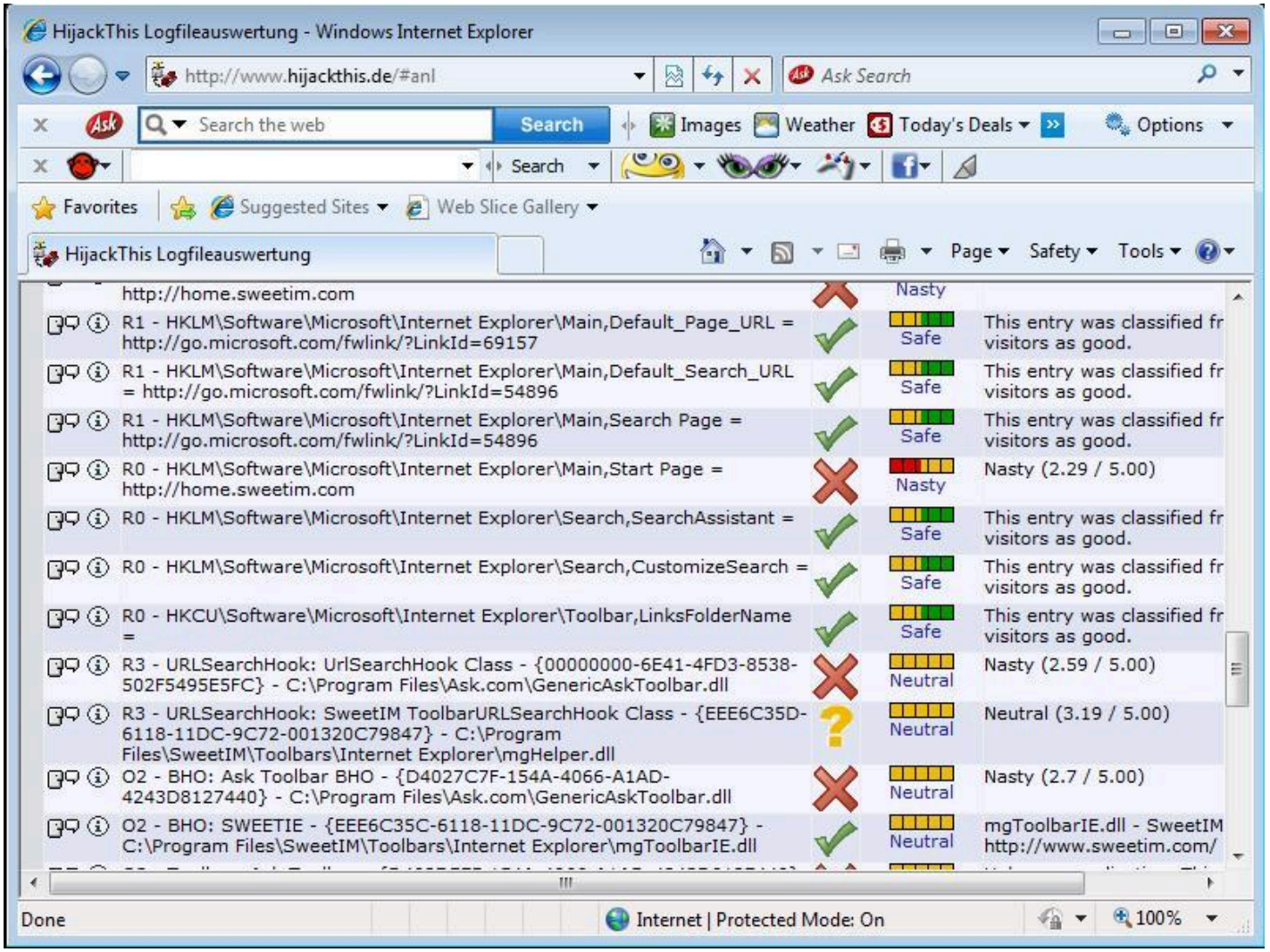
او المفكرة قم بتحديد كل شي note اختر الخيار الاول وبعد عملية الفحص سوف تنبثق لك بها وقم بعملية نسخ

ثم نتوجة الى موقع يقوم بتحليل المعطيات وهو

http://www.hijackthis.de



نقوم بلصق المعطيات التي نسخناه في المربع ونطلب التحليل



بعدها سيحولنا على النتائج وعلامة الصح تعني انه لامشكلة والاستفهام تعني لم يستطيع تحديد اذا كان برنامج ضار او لا وعلامة الاكس الحمراء تعني انه برنامج ضار يجب التخلص منه اما بستخدام مكافح فيروسات او بطريقة يدوية

cnet رابط تحميل البرنامج من موقع

http://download.cnet.com/Trend-Micro-HijackThis/3000-8022_4-10227353.html

---

لكشف تلغيم ملف او برنامج او حقن ملفات وملحقات النظام استخدم برنامج او موقع

threatexpert

صورة من البرنامج

الشرح ينقسم لقسمين شرح الموقع في القسم الثاني

لتحميل البرنامج من موقعه الرسمي

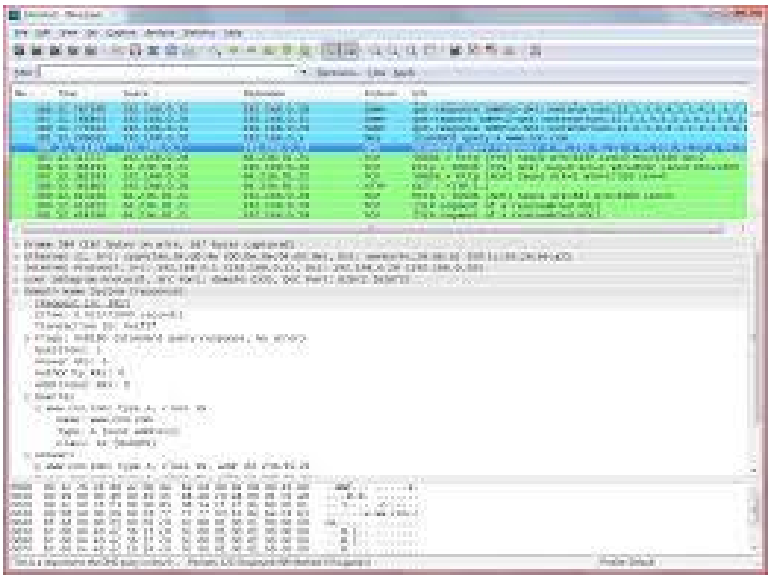
الشرح كامل وشرح الموقع في نصف الفديو

كشف الاختراق ثم تتبع المخترق والحصول على بيانتة واين موقعة

اذا ما شككت بانك تعرضت للاختراق عليك بجمع معلومات الاتصال التي تخرج من جهازك وهناك برنامج يقوم بجمع كل الاتصالات التي تخرج من جهازك

wireshark

وبعد جمعها نقوم بالبحث عن عنواين اسمية عبر الدي ان اس لان الهكر يستخدم اسلوب الاتصال العكسي لئن رقم الاي بي ليس ثابت لذالك يستخدم عنوان اسمي ثابت على غرار عناوين المواقع العادية التي تحمل عنواني اسمي وليس رقمي هنالك العديد من عناوين الشركات التي تقدم خدمة الاتصال العكسي ساضعها في الاسفل لتقوم بالبحث عنها في اتصالات جهازك عبر البرنامج و وجدت شرح في اليوتيوب ممتاز يقدمة شاب مغربي روابط تحميل البرنامج والشرح في الاسفل



[لتحميل الرنامج من الموقع الرسمي]

[الشرح من هنا]

مفاتيح التفعيل

-FA5XU-F7XE2-488XY-UDWEC-XPKRF
-ZZ5D2-FGF44-M89QP-VPXNX-QUHEA
-CV3WA-DEG94-08EGP-C4QNE-P32ZA
-GY71R-4CY55-08D5Y-37QZE-NQKT4
-VG50H-0WDD6-084VQ-UPPGE-ZC8RF
-YV3HK-47Z01-M85QZ-0NQXZ-ZGKYF
-AC5RH-49W07-M84CQ-LQZQT-ZP0CF
-GA5JK-0DG94-08DGP-FYQGZ-MU0FF

عناوين اسمية يستخدمها الهكرز لعمل الاتصال العكسي ابحث عنها في اتصال شبكة اتصال جهازك كما في الشرح

3utilities.com
bounceme.net
ddns.net
ddnsking.com

ddnsking.com
gotns.ch
hopto.org
myftp.biz
myftp.org
myvnc.com
no-ip.biz
no-ip.info
no-ip.org
noip.me
redirectme.net
servebeer.com
serveblog.net
servecounterstrike.com
serveftp.com
servegame.com
servehalflife.com
servehttp.com
serveminecraft.net
servemp3.com
servepics.com
servequake.com
sytes.net
webhop.me
zapto.org

وان شككت في ملف او رابط ارفعه لفيروس توتال لكي يفحص ويعطيك النتيجة

https://www.virustotal.com/ar/

كشف البرامج التي تعمل على في الخفاء او خلفية الجهاز

الهكر يقوم بحقن برنامج عادي بملف يسمى الباتش او السيرفر او باك دور او تروجان كلها اسماء لنفس الاداة وعندما يقوم بعملية الدمج او الحقن في برنامج معين وبعد ان تقوم بتشغيله يعمل بشكل طبيعي ثم يعمل التروجان في الخلفية بدون علمك ولكشف هذا التروجان ولتحديد مكانه استخدم برنامج

Process Explorer

دقق في العمليات التي تحمل اللون الازرق وان لاحظت وجود برنامج لم تقوم انت بتنصيبة او تشغيلة اعملة كيل بروسيسر لايقاف عملة و لقطع اتصاله بلانترنت ثم اتبع مسار الملف وارفعة لموقع التحليل وانتظر النتيجة على الايميل وتصل في مده اقصها ساعة في وقت ذروة الذروة والضغط

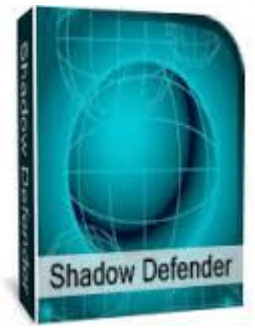
للتحميل من موقع ميكروسوفت الرسمي هنا

---

* برامج تجميد النظام

وانصح بستخدام برامج تجميد النظام بحيث لوتعرضت للاختراق التصق التروجان بجميع مللفاتك ماعليك الا عمل ريستارت للجهاز ويعود كما كان وهناك برنامجين انصح بهم

shadow defender



لتحميل من هنا

او برنامج ديب فريز الشهير

deep freeze

لتحميل من هنا

---

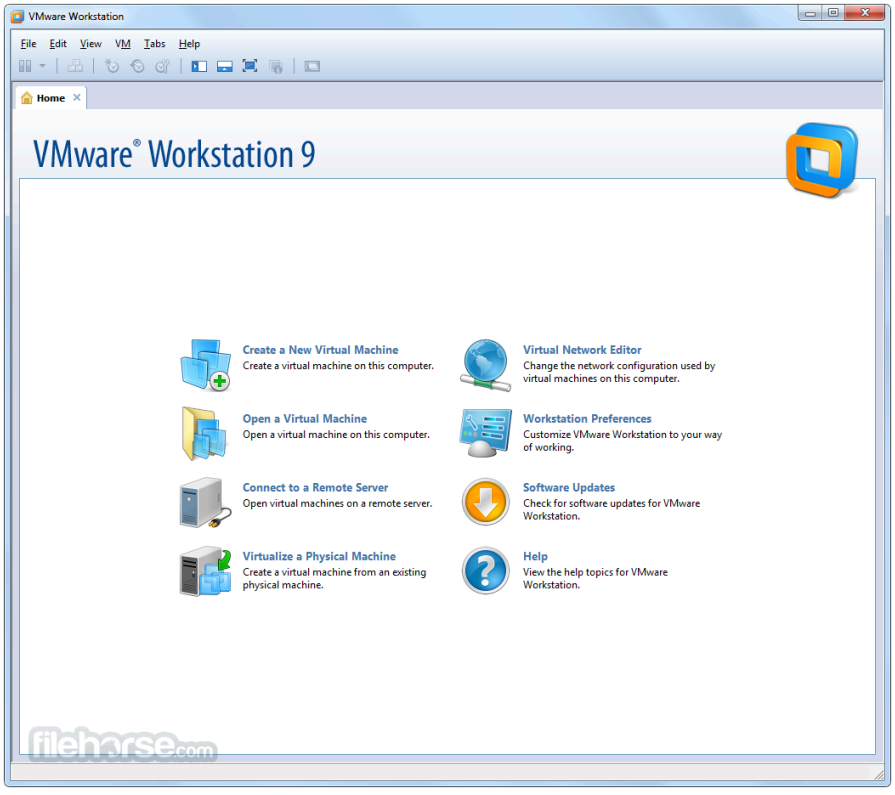
* برامج البيئة الوهمية

لعمل نظام وهمي داخل النظام الحقيقي مثال اذا انت نظامك ويندوز 7 وتريد تنصيب نظام ماك من ابل داخل نظام الوندوز وعمل جهاز وهمي استخدم برنامج

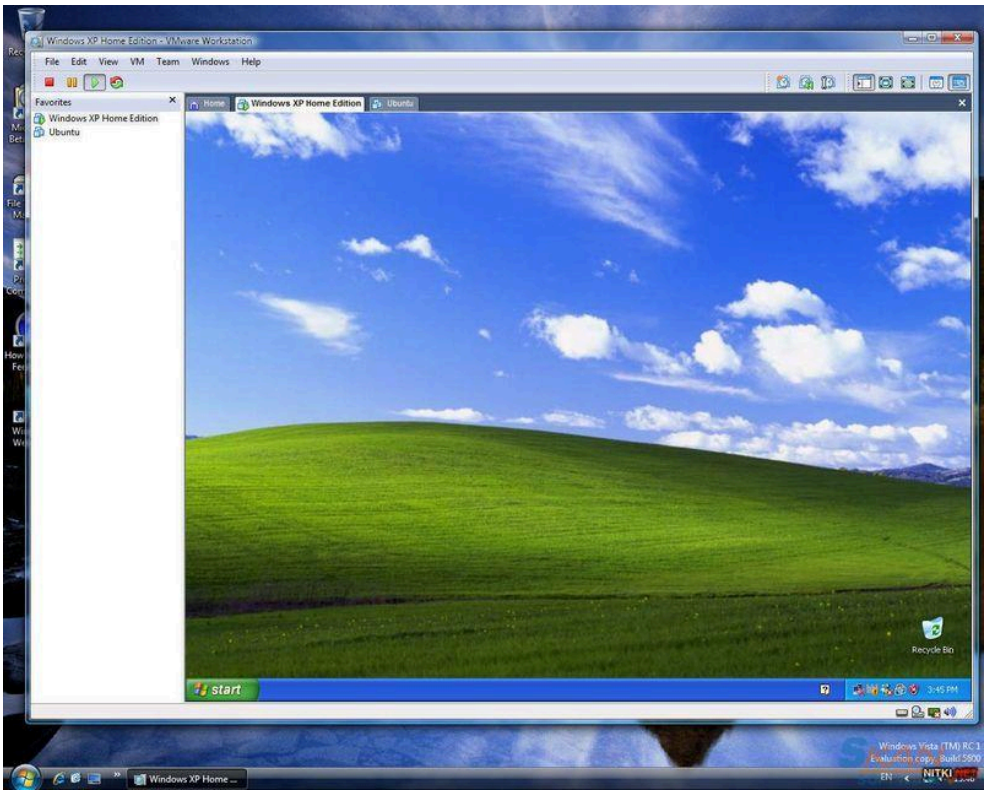
ويندوز 8 يئتي بنظام مدمج مع النظام ولاتحتاج لبرامج خارجية

vmware workstation

وهو سيتكفل بعمل النظام الوهمي بعد ان تقوم بتحميل نسخة من النظام الذي تريد ليكون نظام وهمي لك ويجب مراعاة متطلبات انظمة ابل بالتحديد لكي تعمل على اجهزة من غير شركة ابل



صورة من داخل البرنامج وهو يعمل بنظام وندوز 7 اساسي و وندوز اكس بي وهمي



شرح البرنامج بالفديو عبر اليوتيوب من هنا

لتحميل البرنامج من الموقع الرسمي من هنا

مفاتيح التفعيل

-VF190-AMZEQ-M81UZ-QNM7E-PFUX2

-UZ5TA-29E8L-088RP-U6QQV-QKAY2

-GU3W8-0TXD0-0899Z-D4P79-XK2Z4

-FV1M0-06Y11-08DMP-Z6QZG-ZC8V4

-CA1HR-4YG0Q-08DAQ-1QXEC-NG0V2

-ZV1J0-4MZ86-0808P-0YZ5V-P3HT4

-FU7D0-D2GDJ-M89KP-76XGT-NFKWD

-UZ7MR-DXWEP-4891Y-X7MX9-M30T0

-YC3X0-D0G4P-M89DQ-ZMZ59-NZ8R4

-UA3MR-ARX5Q-H89QZ-AYYGE-N6094

-YU5XA-FJX42-M88MY-T4PNG-YP094

-AA5MR-03G4N-H84JY-06XGZ-ZYAFD

-AV7NU-0DG9Q-088TY-M7XEC-NU8GF

-UA7H0-4TF12-484CP-RXWE9-WK8R4

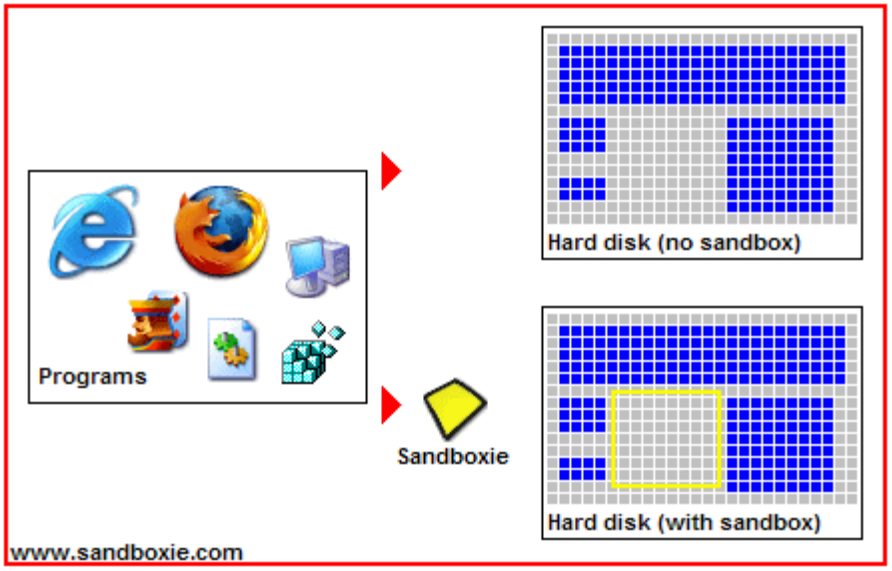
-YG7MR-09Y52-0889Q-EPM5Z-NGKD4

برنامج البيئه الوهمية اي ان الملف المشكوك به يتم تشغليه بواسطة البرنامج وعند اغلاق النافذه يبقى الجهاز على حالة حتى لو ان الفيروس من اشد الفيرسات لن يؤثر على الجاهز

اسم البرنامج

Sandboxie

طريقة عمل البرنامج



لتحميل من هنا

*امن الاتصالات الهاتفية GSM و الهواتف المشفرة

هناك خدمات اتصلات مشفرة مقدمة من شركات متخصصة بالتشفير وهذه الهواتف لا يمكن التجسس عليها

وهو هاتف يعمل بنظام اندرويد ويحمل برامج اتصال هاتفي وتراسل كتابي مشفرة

هاتف blackphone

لشراء الهاتف تفضل بزيارة موقع الشركة على هذا الرابط

https://www.blackphone.ch/

* برامج اتصال هاتفي مشفرة

Silent Circle

هي شركة تقدم هاتف بلاك فون او البرامج المستخدمة في تشفير البلاك فون على منصة ابل و اندرويد ويلزم اشتراك شهري

رابط البرامج من الشركة ولو قمت بالبحث عن البرامج في المتجر ستجدها ايظن

https://silentcircle.com/#apps

اعداد : عمروف الجلاد

JladOmarov@

http://ask.fm/Sir_masool2