



بسم الله الرحمن الرحيم

آخر 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 ما يحدث في الارض واغلاق الحسابات المتكرر على تويتر لاشك ان امن اتصالاتك مهم ولهذا قمت باعداد هذا الشرح القديم المجدد تشفير الاتصال . تشفير الجهاز كامل اجزاء من الهارديسك او) بشكل مفصل ويشمل الشرح ملف معين . تشفير اتصال الهاتف الجوال . خدمة البريد الالكتروني 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 وساقوم باضافة بعض النقاط بتعديل على (تحليل برامج الجهاز باستخدام هيجاك . DNS نفس هذه الصفحة في وقت لاحق ان شاء الله لزيادة المعلومات

اعداد : عمرو الجاد

JladOmarov@

ask.fm

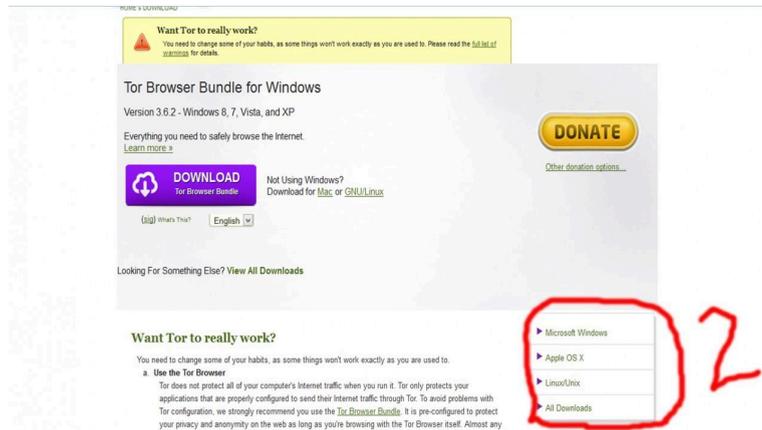
تشفير اتصالاتك واستخدام شبكات التور و الفي بي ان

لمن يستخدم نظام 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 و نصب البرنامج ستظهر لك هذه الاليقونة على سطح المكتب انقر عليه لتشغلها وسيفتح معك متصفح خاص بالشبكة



عند فتح البرنامج سيتم الاتصال خلال ثواني بسر افرات شبكة التور وسيفتح متصفح فاير فوكس خاص بشبكة تور يقوم بمسح كل مخلفات التصفح



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

اصحاب الالفون والايباد و الجالکسي

لا يوجد برنامج تور للالفون 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

[Freedom](#)

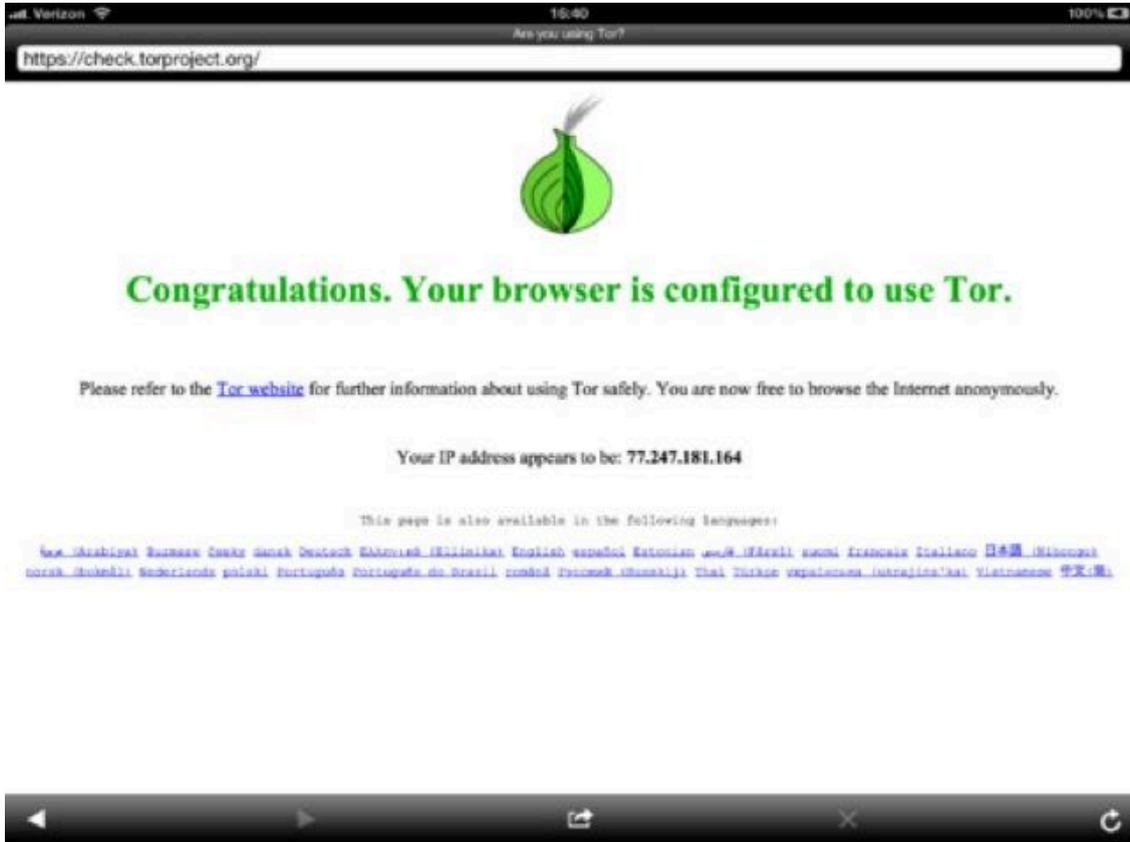
اندرويد

freedom.vpn

***المتصفحات الامنة والمشفرة للايفون و اندرويد**

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

متصفح onionbrowser



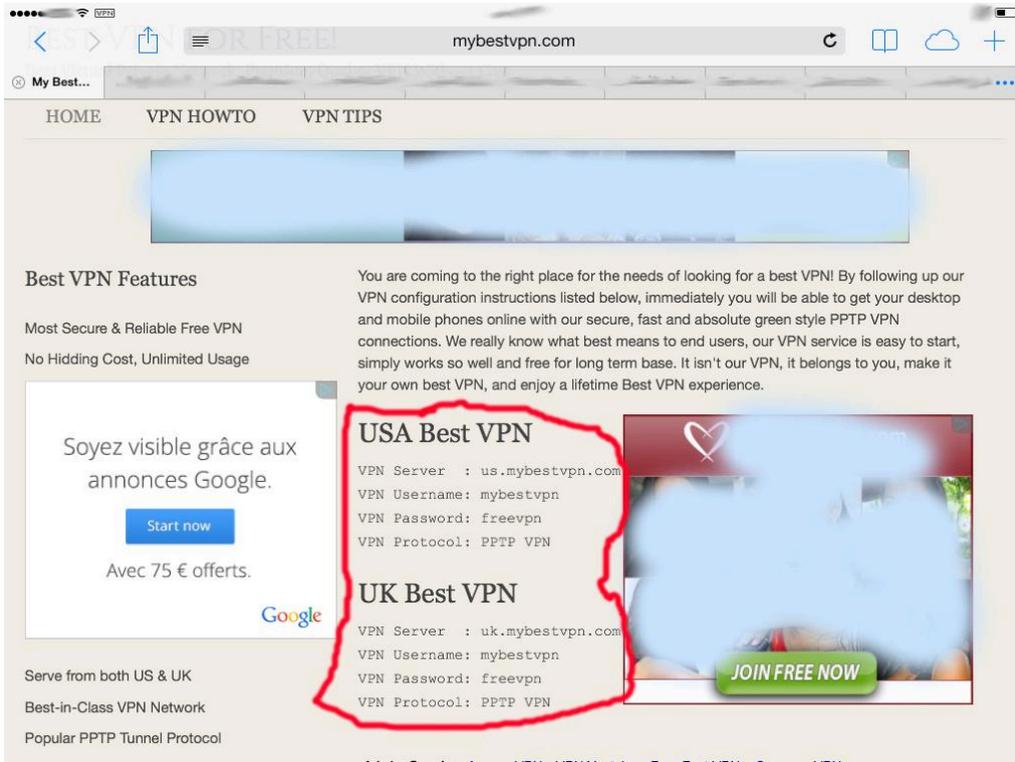
للتحميل من ابل ستور الخاص بالآيفون [هنا](#)

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

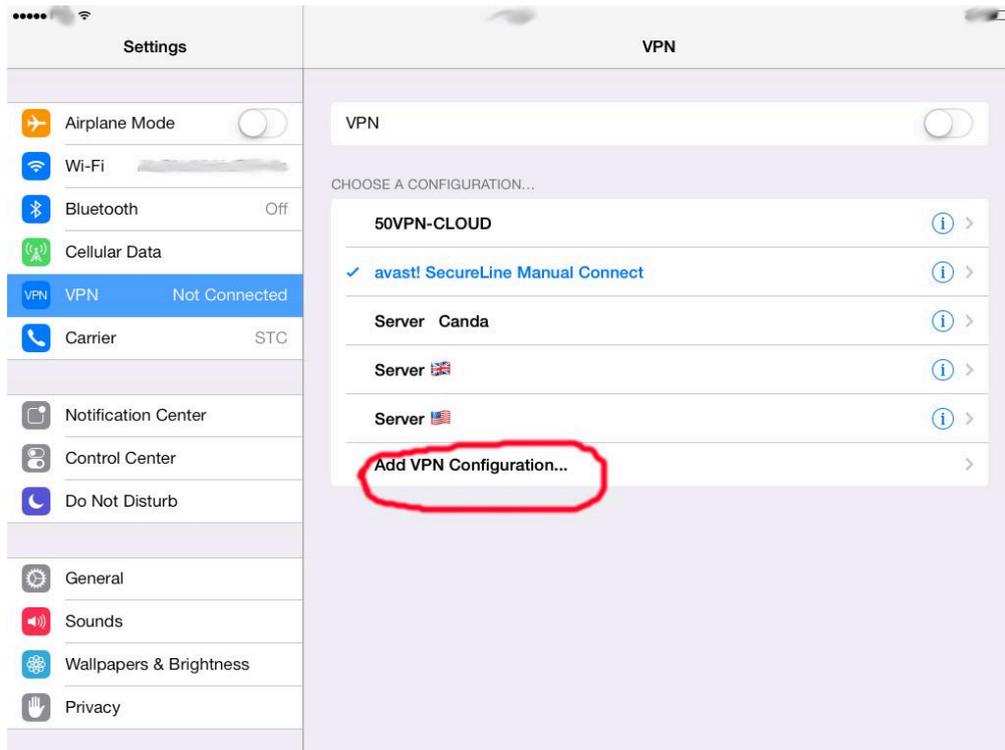
ادخل على هذا الرابط مع العلم انه محجوب لكن ساضع لكم بيانات شبكة في بي ان في اخر الموضوع

ادخل على هذا الرابط

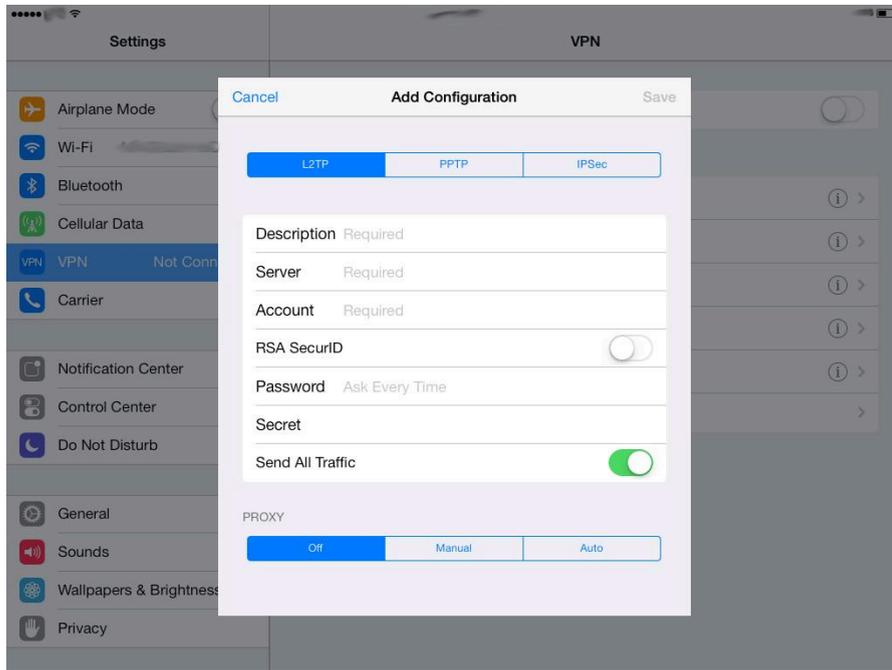
<http://mybestvpn.com/>



اختر احد السيرفرات وخذ البيانات ثم نروح لعدادت الالفون او اليبايد



الان نضع البيانات الي اخذناها حسب برتكول الشبكة ونشغل الفاي 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 بتغيير الموقع الجغرافي للصورة بحيث تظهر عند تحليلها من اجهزة الامن انها ملتقطة في اي بلد انت تختاره وانصح باستخدام برنامج

Photo GPS Editor

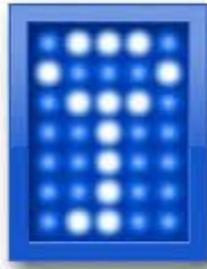
لسهولة استخدامة



*** تشفير الأجهزة بالكامل او جزء من الهارديسك**

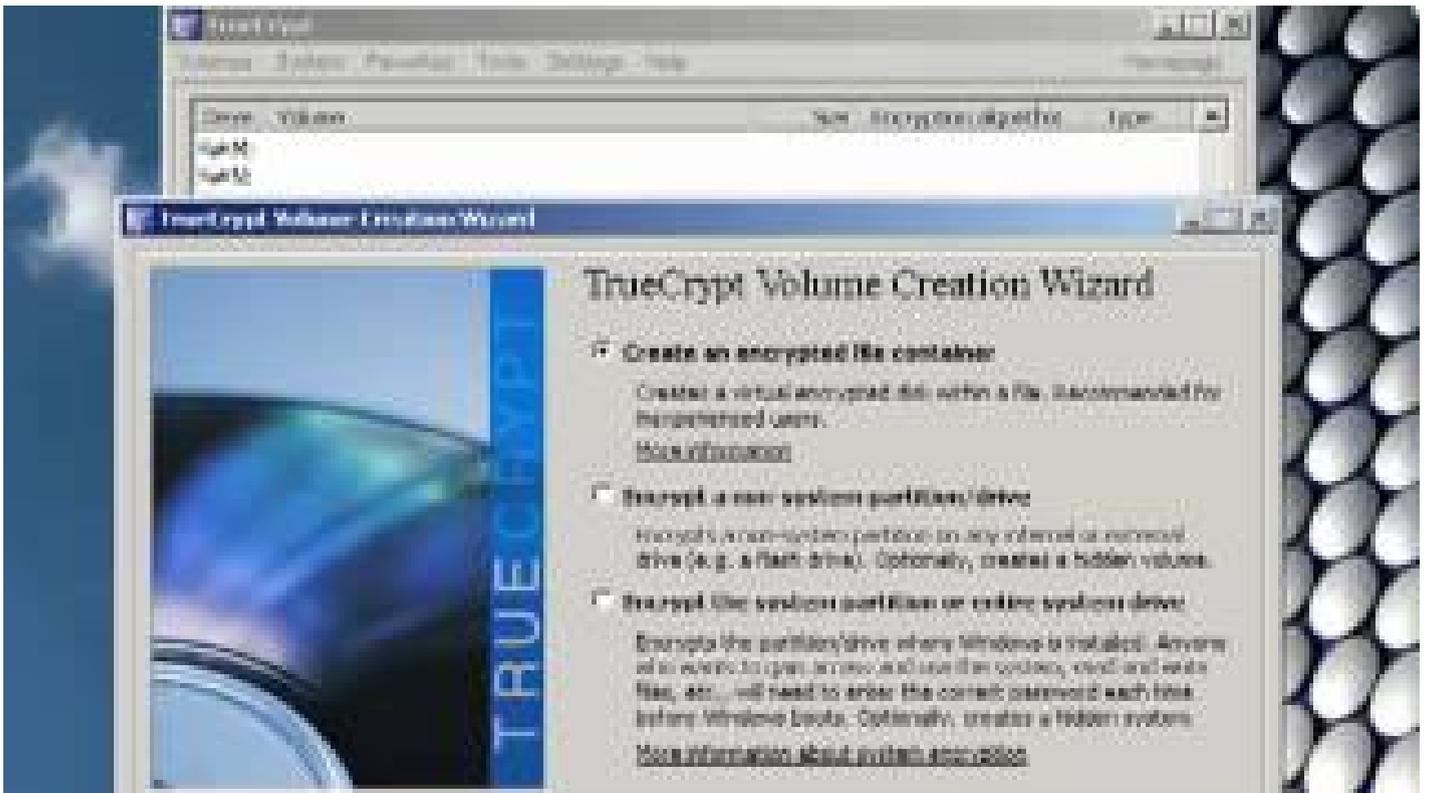
لتشفير جهازك بالكامل او جزء من الهارديسك او ملف معين مهما كان انصحك باستخدام هذا البرنامج

True Crypt لتحميل اضغط على [هنا](#)



TrueCrypt

شرح البرنامج فيديو



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



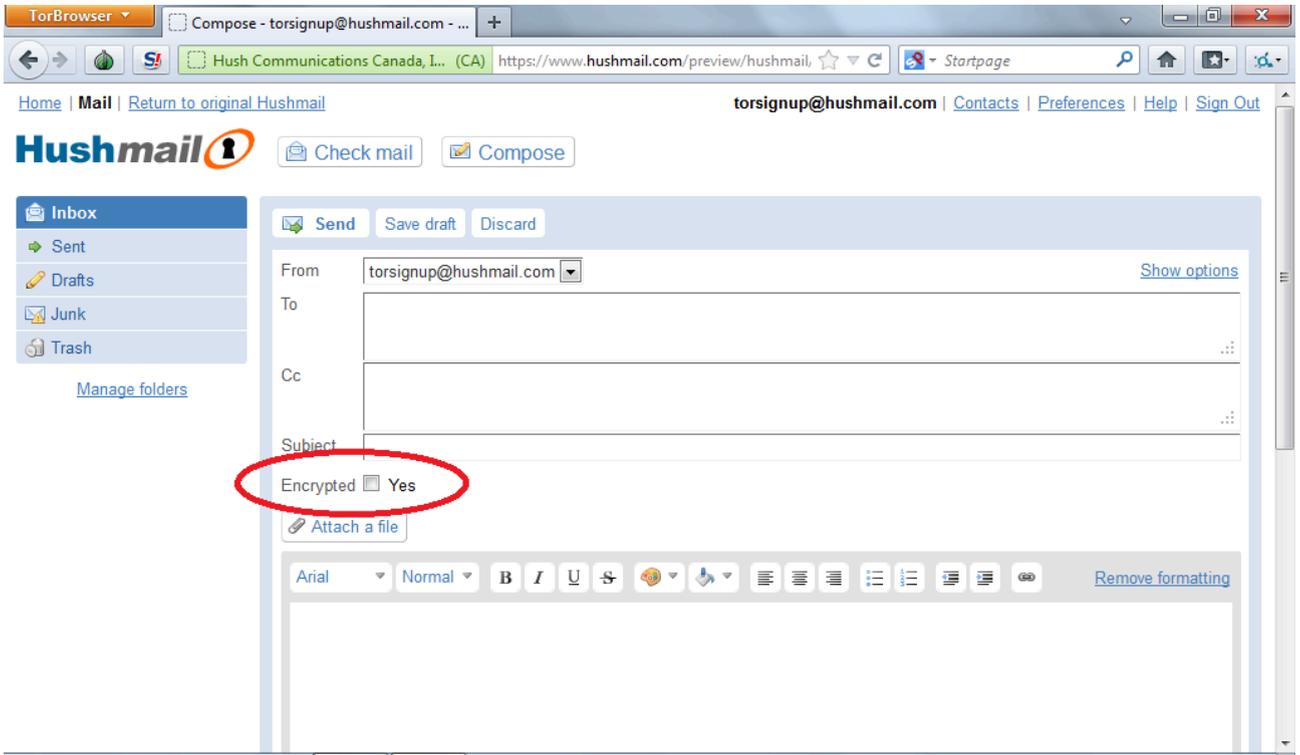
***البريد الالكتروني المشفر بالكامل**



لتسجيل في الخدمة من [هنا](#)

خدمة كندية عالية التشفير





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 عليه والهكر ايظن عن طريق التنصت على الشبكة وحين تكتب رسالة تظهر من غير تشفير للهكر

البديل هو برنامج Telegram الذي يحتوي على خدمة التحدث المشفر الامن



تحميل البرنامج للآيفون 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 عليه



لتحميل البرنامج للآيفون من [هنا](#)

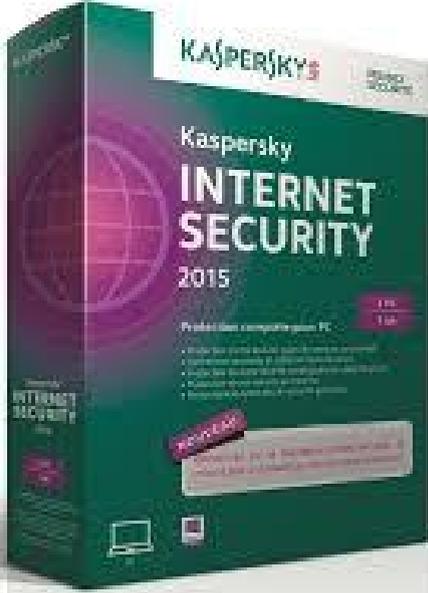
لتحميل البرنامج للاندرويد من [هنا](#)

* برامج الحماية

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

انصح بالذب الروسي برنامج

kaspersky internet security 2015

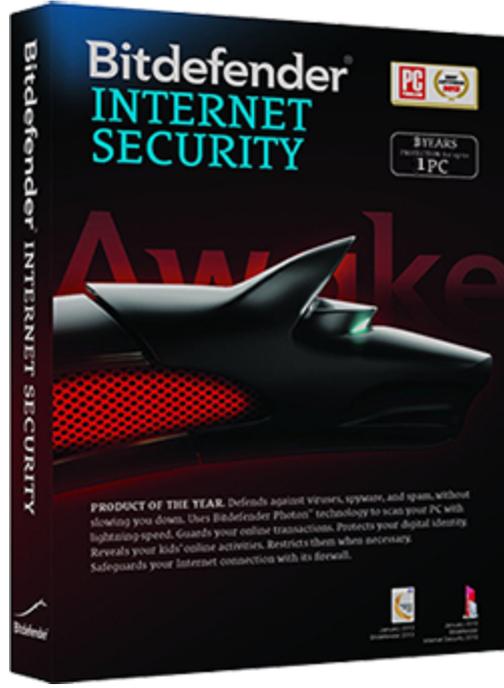


لشراء البرنامج من [هنا](#)

برنامج خارق يقدم الحماية القصوى

العلاق 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

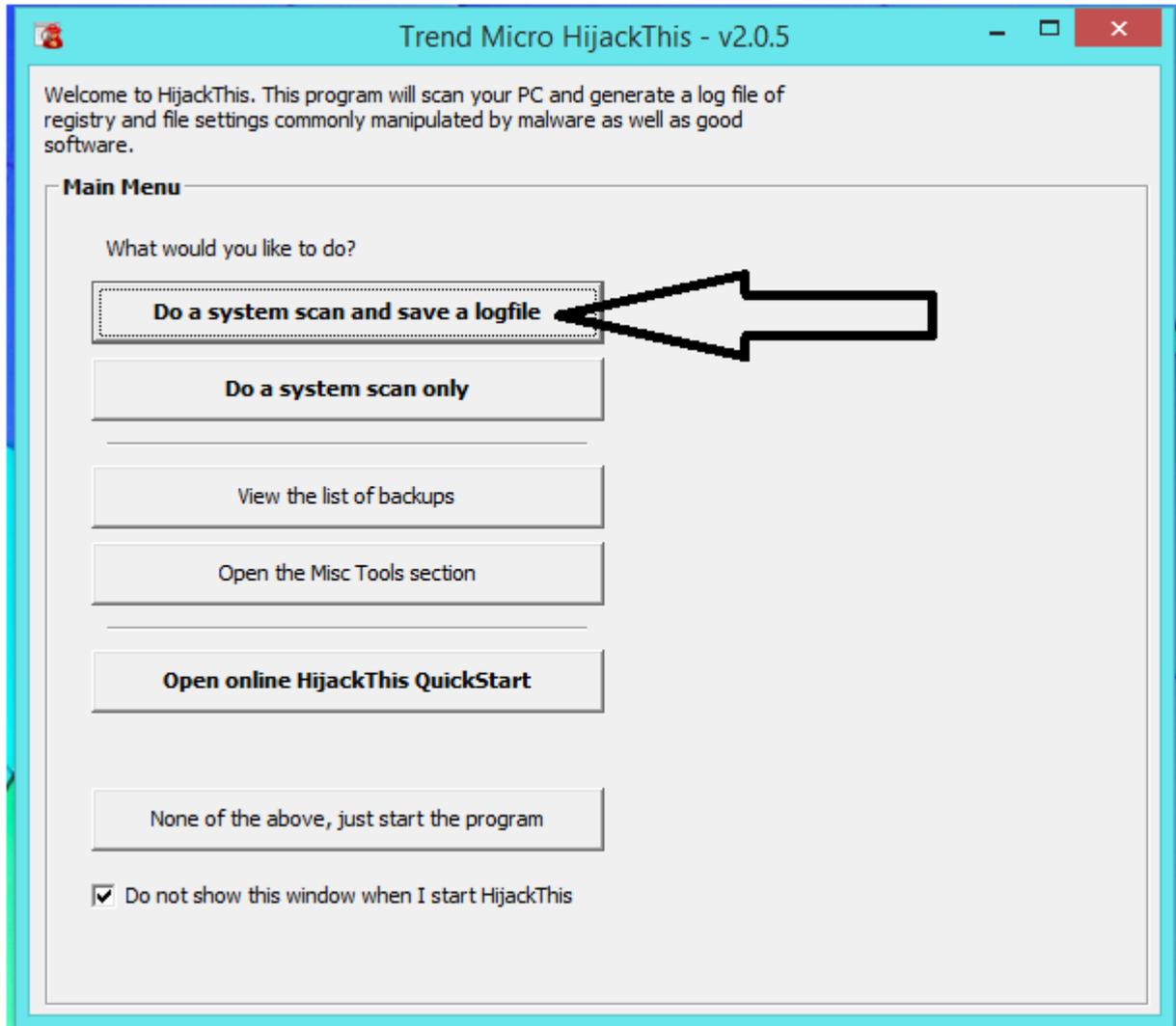
تنتهي في تاريخ 26 \ 7 \ 2017

*تحليل الملفات وكشف التلغيم

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



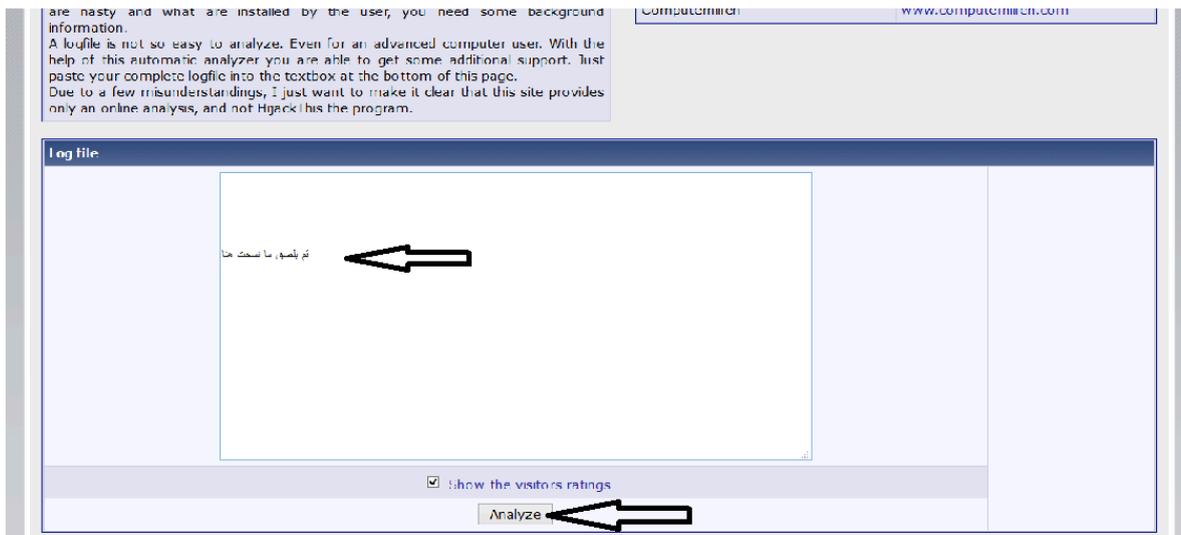
شغل الاداة كمسؤول ثم وافق على الاتفاقية



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

ثم نتوجه الى موقع يقوم بتحليل المعطيات وهو

<http://www.hijackthis.de>



نقوم بلصق المعطيات التي نسخناه في المربع ونطلب التحليل

HijackThis Logfileauswertung - Windows Internet Explorer

http://www.hijackthis.de/#anl

Search the web | Search | Images | Weather | Today's Deals | Options

HijackThis Logfileauswertung

http://home.sweetim.com	✗	Nasty	
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/fwlink/?LinkId=69157	✓	Safe	This entry was classified fr visitors as good.
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896	✓	Safe	This entry was classified fr visitors as good.
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896	✓	Safe	This entry was classified fr visitors as good.
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://home.sweetim.com	✗	Nasty (2.29 / 5.00)	
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =	✓	Safe	This entry was classified fr visitors as good.
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =	✓	Safe	This entry was classified fr visitors as good.
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =	✓	Safe	This entry was classified fr visitors as good.
R3 - URLSearchHook: UrlSearchHook Class - {00000000-6E41-4FD3-8538-502F5495E5FC} - C:\Program Files\Ask.com\GenericAskToolbar.dll	✗	Neutral	Nasty (2.59 / 5.00)
R3 - URLSearchHook: SweetIM ToolbarURLSearchHook Class - {EEE6C35D-6118-11DC-9C72-001320C79847} - C:\Program Files\SweetIM\Toolbars\Internet Explorer\mgHelper.dll	?	Neutral	Neutral (3.19 / 5.00)
O2 - BHO: Ask Toolbar BHO - {D4027C7F-154A-4066-A1AD-4243D8127440} - C:\Program Files\Ask.com\GenericAskToolbar.dll	✗	Neutral	Nasty (2.7 / 5.00)
O2 - BHO: SWEETIE - {EEE6C35C-6118-11DC-9C72-001320C79847} - C:\Program Files\SweetIM\Toolbars\Internet Explorer\mgToolbarIE.dll	✓	Neutral	mgToolbarIE.dll - SweetIM http://www.sweetim.com/

Done | Internet | Protected Mode: On | 100%

بعدها سيحولنا على النتائج وعلامة الصح تعني انه لامشكلة والاستفهام تعني لم يستطيع
تحديد اذا كان برنامج ضار او لا وعلامة الكس الحمراء تعني انه برنامج ضار يجب التخلص
منه اما باستخدام 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 الفيديو](#)

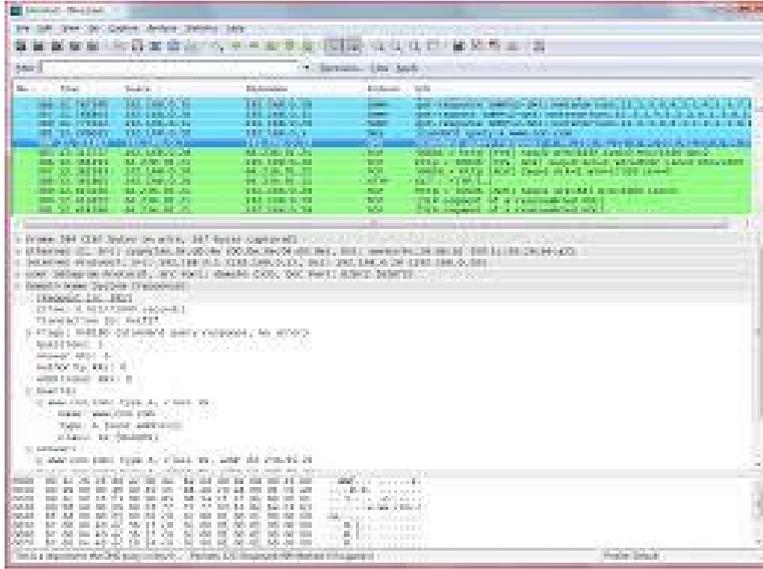
كشف الاختراق ثم تتبع المخترق والحصول على بيانته واين موقعة

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 عناوين اسمية عبر الذي ان اس لان الهكر يستخدم اسلوب الاتصال العكسي لنن رقم الاي بي ليس ثابت لذلك 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 يقدمه شاب مغربي روابط تحميل البرنامج والشرح في الاسفل





لتحميل البرنامج 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 الهكز 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
zapro.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

Process	PID	CPU	Description	Company Name	Start Time	Virtual Size	Working Set	Private Bytes
svchost.exe	3232				10:38:21 2009-12-...	24,340 K	1,808 K	
taskhost.exe	3968		Host Process for Windows T...	Microsoft Corporation	10:38:52 2009-12-...	65,684 K	3,448 K	
SearchIndexer.exe	3576				10:39:02 2009-12-...	223,180 K	34,736 K	
SearchProtocolHost.exe	5484				16:52:09 2009-12-...	71,944 K	4,844 K	
SearchFilterHost.exe	4904				18:59:13 2009-12-...	23,440 K	3,688 K	
iPodService.exe	128				10:39:06 2009-12-...	39,768 K	1,884 K	
taskhost.exe	3076				11:23:13 2009-12-...	76,376 K	1,272 K	
lsass.exe	584				10:38:07 2009-12-...	36,424 K	5,628 K	
lsass.exe	592				10:38:07 2009-12-...	25,072 K	1,960 K	
csrss.exe	524				10:38:07 2009-12-...	240,024 K	32,072 K	
conhost.exe	6224		Console Window Host	Microsoft Corporation	16:49:18 2009-12-...	34,392 K	2,828 K	
winlogon.exe	688				10:38:08 2009-12-...	40,116 K	1,656 K	
processp.exe	6356	0.38	Sysinternals Process Explorer	Sysinternals - www.sysinter...	18:59:13 2009-12-...	103,416 K	22,316 K	
explorer.exe	1428	0.38	Windows Explorer	Microsoft Corporation	10:38:53 2009-12-...	292,908 K	56,424 K	
AvastUI.exe	2820		avast! Antivirus	ALWIL Software	10:38:54 2009-12-...	80,692 K	2,784 K	
RtHDVCpl.exe	2832		HD Audio Control Panel	Realtek Semiconductor	10:38:55 2009-12-...	89,244 K	1,588 K	
UpdaterUI.exe	2940		Common User Interface	McAfee, Inc.	10:38:55 2009-12-...	78,012 K	2,160 K	
McTray.exe	3724		McAfee Security Agent Task...	McAfee, Inc.	10:38:55 2009-12-...	53,072 K	364 K	
shstat.exe	3088				10:38:55 2009-12-...	79,128 K	860 K	
iTunesHelper.exe	512		iTunesHelper	Apple Inc.	10:38:55 2009-12-...	112,648 K	2,440 K	
javasched.exe	3688		Java(TM) Platform SE binary	Sun Microsystems, Inc.	10:38:55 2009-12-...	53,376 K	948 K	
GoogleUpdate.exe	1460		Google Installer	Google Inc.	10:38:56 2009-12-...	56,296 K	2,096 K	
GoogleCrashHandler.exe	3840		Google Installer	Google Inc.	10:38:56 2009-12-...	50,436 K	1,040 K	
PrintScreen.exe	2144		Gadwin PrintScreen	Gadwin Systems, Inc.	10:38:56 2009-12-...	130,128 K	13,768 K	
pidgin.exe	3508		Pidgin	The Pidgin developer com...	10:46:29 2009-12-...	161,980 K	27,240 K	
LastFM.exe	952		Last.fm	Last.fm	10:47:23 2009-12-...	142,828 K	2,616 K	
firefox.exe	4272	3.46	Firefox	Mozilla Corporation	10:50:25 2009-12-...	1,191,804 K	509,616 K	
javazuncher.exe	5164		Java(TM) Platform SE binary	Sun Microsystems, Inc.	16:49:18 2009-12-...	48,048 K	3,304 K	
java.exe	1116		Java(TM) Platform SE binary	Sun Microsystems, Inc.	16:49:18 2009-12-...	358,904 K	80,424 K	
thunderbird.exe	4984	0.38	Thunderbird	Mozilla Messaging	10:51:44 2009-12-...	290,164 K	113,564 K	
chrome.exe	4188		Google Chrome	Google Inc.	11:18:51 2009-12-...	249,568 K	57,144 K	
chrome.exe	1896		Google Chrome	Google Inc.	11:18:51 2009-12-...	113,648 K	4,676 K	

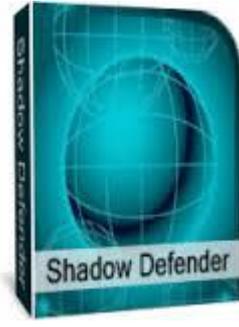
دقق في العمليات التي تحمل اللون الازرق وان لاحظت وجود برنامج لم تقوم انت بتنصيبه او تشغيله اعملة كيل بروسيسر لايقاف عملة و لقطع اتصاله بالانترنت ثم اتبع مسار الملف وارفعة لموقع التحليل وانتظر النتيجة على الايميل وتصل في مده اقصها ساعة في وقت ذروة الذروة والضغط

[للتحميل من موقع ميكروسوفت الرسمي هنا](#)

* برامج تجميد النظام

وانصح باستخدام برامج تجميد النظام بحيث لو تعرضت للاختراق التصق التروجان بجميع ملفاتك ما عليك 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](#)

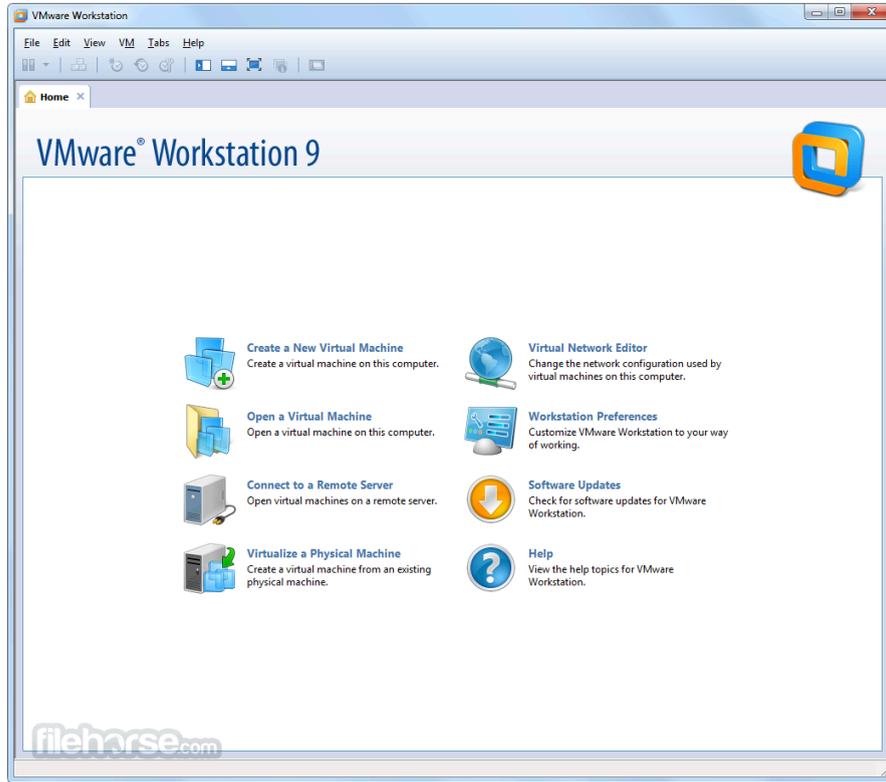
* برامج البيئة الوهمية

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

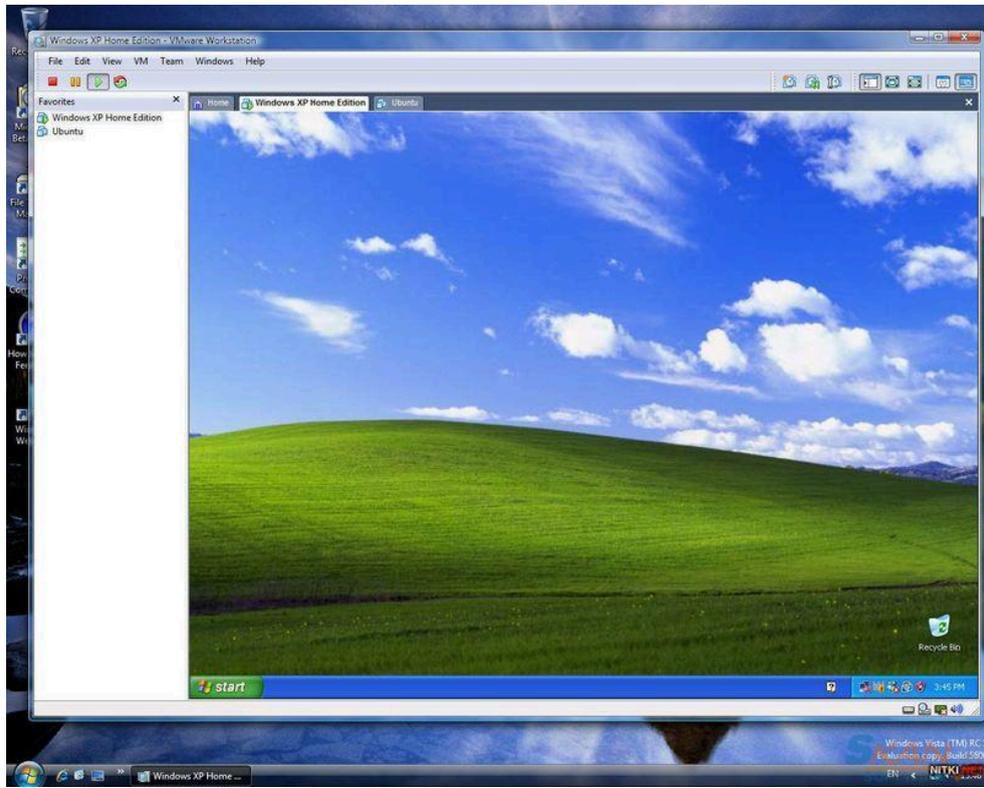
ويندوز 8 ييتي بنظام مدمج مع النظام ولاتحتاج لبرامج خارجية

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 بالفيديو 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

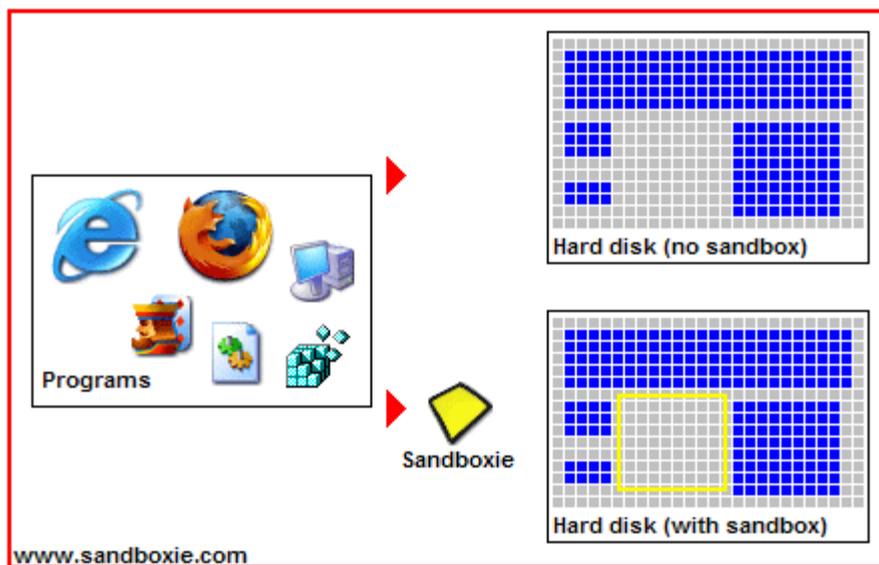
برنامج البيئه الوهمية اي ان الملف المشكوك به يتم تشغيله بواسطة البرنامج وعند اغلاق النافذه يبقى الجهاز على حالة حتى لو ان الفيروس من اشد الفيروسات لن يؤثر على الجهاز

اسم البرنامج

Sandboxie



طريقة عمل البرنامج



لتحميل من [هنا](#)

*امن الاتصالات الهاتفية GSM و الهواتف المشفرة

هناك خدمات اتصالات 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 الجناد

JladOmarov@

http://ask.fm/Sir_masool2