مدونة شمس
www.freecccam.org

كتاب شرح برنامج تور

TOR

مدونة الشوقية

www.freecccam.org

freecccamorg@gmail.com

اهداء الى المجاهدين في سوريا الحبيبة والاحواز المحتلة
من العدو المجوس الفارسي

2011

وشكر خاص للإخوان الكرام في شبكة شموخ الاسلام والتحدي والفلوجة وانصار المجاهدين

واقول لكم بارك الله فيكم وجعل الله اعمالكم المباركة الطيبة في موازين حسناتكم

اللهم انصر المجاهدين في سوريا وفى الاحواز وفى العراق

المؤلف :	مشروع تور
الإصدار الأولي:	20 سبتمبر 2003
آخر إصدار :	2011 /1.3.24
مكتوب بلغة:	سي
نظام تشغيل:	متعدد المنصات
النوعية:	تخفي
الترخيص:	رخصة بي إس دي

موقع وب: www.torproject.org

تور (بالإنجليزية: **Tor**) اختصارًا لـ (**The Onion Router**) هو برنامج تخفي على شبكة الإنترنت يعتمد الجيل الثاني من نظام التوجيه البصلي وهو نظام يمكن مستخدميه من الاتصال بدون الكشف عن الهوية على شبكة الإنترنت.

قدم روجر دينجليدين، ونيك ماثيوسن، وباول سيفيرسون نظام تور في الندوة الأمنية الثالثة عشر لاتحاد الحوسبة التقنية المتقدمة

تلميحه عن تور

تور هو عبارة عن شبكة من الأنفاق الافتراضية التي تتيح للأفراد والجماعات التصفح بخصوصية وأمان على الإنترنت. كما أنها تمكن مطوري البرمجيات من صنع وسائل اتصال جديدة تحمي خصوصية مستخدميها. تور يوفر القاعدة لمجموعة من البرامج التي تسمح للمؤسسات والأفراد تبادل المعلومات عبر الشبكات العامة دون المساس خصوصياتهم.

يستخدم برنامج تور لمنع مواقع الويب من تتبع متصفحيها أو أفراد أسرهم ، أو لتصفح مواقع الأخبار ، وخدمات المراسلة الفورية أو الشات ، أو ما شابه ذلك عندما يتم حظرها من قبل مزودي خدمات الإنترنت . يسمح الخدمات المخفية تور للأشخاص تحميل المواقع على الإنترنت وغيرها من الخدمات دون الحاجة إلى الكشف عن موقعهم. يستخدم تور أيضا للقيام بمحادثات على مواضيع حساسة اجتماعيا : مثلا غرف الدردشة والمنتديات التي يستخدمها الناجون من الاغتصاب والاعتداء الجنسي ، أو الناس الذين يعانون من أمراض معينة.

يستخدم الصحفيون و المدونون تور للاتصال بأمان مع ناشري الأسرار و المعارضين. كما تقوم المنظمات غير الحكومية (الان جي اوز) باستخدام تور للسماح لعامليها بالتواصل مع مواقعهم الأم حينما يكونون في بلد آخر، دون إخطار من حولهم بأنهم يعملون مع مؤسسة ما.

توصي مجموعات مثل انديميديا باستخدام تور لحماية خصوصية أعضائها على الانترنت.

المجموعات الناشطة مثل مؤسسة الحدود الإلكترونية (اي اف اف) توصي أيضا باستخدام تور كآلية للدفاع عن الحريات المدنية على الانترنت. تستخدم الشركات تور كطريقة آمنة لإجراء تحليل المنافسين ، و من أجل حماية المشتريات الحساسة من الجواسيس. هم أيضا استخدامه لاستبدال الشبكات الافتراضية المحمولة التي تكشف عن وقت و مكان الاتصال. و ماذا بالنسبة

لمن لديهم موظفون يعملون لوقت متأخر؟ ما هي الفروع التي يبحث موظفوها عن وظائف أخرى؟ و ما هي أقسام البحوث التي تقوم بالتواصل مع محامي الشركة؟

تستخدم فرع من البحرية الامريكية تور لجمع المعلومات الاستخبارية الغير مخفية، وتم استخدام تور منذ فترة قريبة في الشرق الأوسط من قبل إحدى وحداتها.
تستخدم أيض بعض وحدات الشرطة تور من اجل عدم ترك أثر أو عناوين آي بي للمواقع التي يزورونها.

إن تنوع مستخدمي تور هو في الواقع جزء مما يجعلها آمنة جدا . ما يجعل استخدام تور غاية في الأمان المستخدمين الآخرين على الشبكة ، وبالتالي فإن تور يخفيك من المستخدمين الآخرين على الشبكة بحيث كلما كان هناك عدد اكبر من المستخدمين على الشبكة، كلما اصبحت مجهولا أكثر.

لماذا نحن بحاجة لتور

استخدام تور يحميك من شكل شائع من أشكال مراقبة الإنترنت والمعروف باسم "تحليل حركة المرور". ويمكن استخدام تحليل حركة المرور لاستنتاج من يتحدث مع من على شبكة عمومية. معرفة المصدر والمقصد من خلال زيارتك للمواقع على الإنترنت الخاص بك يسمح للآخرين بتعقب سلوكك واهتماماتك. يمكن أن يؤثر هذا على ما تدفعه ، على سبيل المثال ، اذا كان موقع التجارة الإلكترونية يغير الأسعار استنادا إلى بلدك أو مؤسسة المنشأ. ويمكن أن تهدد حتى وظيفتك وسلامتك من خلال الكشف عن هويتك و أين تقيم. على سبيل المثال ، إذا كنت مسافرا في الخارج ، اتصلت بشبكة الكمبيوتر الخاصة بعملك، فمن الممكن ان تقوم عن غير قصد جنسيتك و المؤسسة التي تعمل معها لأي شخص آخر يراقب الشبكة حتى لو كانت الشبكة مشفرة.

لكن كيف يمكن عمل تحليل حركة المرور؟ تتكون حزم بيانات الانترنت من جزأين : **حمولة البيانات والرأس المستخدم للتوجيه**.

حمولة البيانات

هي كل ما يتم إرساله ، سواء كان ذلك رسالة بريد إلكتروني ، صفحة ويب ، أو ملف صوتي. حتى لو كنت البيانات مشفرة فان تحليل حركة المرور الخاصة بك ستمكن من كشف القدر الكبير حول ما تفعله ، وربما ما تقوله. ذلك لأن تحليل حركة المرور يركز على الرأس ، والتي تفصح عن المصدر والمقصد ، والحجم والتوقيت ، وهلم جرا.

هناك مشكلة أساسية لمن يهتمون بخصوصيتهم ألا و هي أن باستطاعة متلقي اتصالاتك رؤية أنك قد قمت بإرسال شيء من خلال النظر الى الرأس.
كما يستطيع القيام بهذا كل الوسطاء المرخص لهم مثل مزودي خدمات الإنترنت ، والوسطاء الغير مرخص لهم كذلك. نموذج بسيط جدا من تحليل حركة المرور يعني الجلوس في مكان ما بين المرسل و المتلقي على الشبكة و تفحص الرأس أو الرؤوس.

ولكن هناك أيضا أنواع أقوى من تحليل حركة المرور. بعض المهاجمين يتجسسون على أجزاء متعددة من شبكة الإنترنت ، يستخدمون تقنيات إحصائية متطورة لتعقب أنماط الاتصالات التي

تقوم بها العديد من المنظمات المختلفة والأفراد التشفير لا يساعد ضد هؤلاء المهاجمين ، لأنه يخفي فقط محتوى حركة المرور على الإنترنت ، وليس الرؤوس.

الحل: هو شبكة موزعة و مجهولة

يساعد تور على الحد من خطورة تحليل حركة المرور البسيط والمتطور من خلال توزيع المعاملات الخاصة بك على عدة أماكن على الإنترنت ، لذلك لا يمكن لنقطة واحدة فقط أن توصلك إلى وجهتك. الفكرة هنا مشابهة لاستخدام طريق ملتو، يصعب متابعته من أجل التخلص من شخص ما يلاحقك -- ثم يقوم تور بمحو بصماتك بشكل منتظم. بدلا من اتخاذ طريق مباشر من المصدر إلى الوجهة ، تأخذ حزم البيانات على شبكة تور مسارا عشوائية من خلال تبديلات عدة تغطي مساراتك بك بحيث لا يستطيع أي مراقب في أي نقطة أن يحدد من أين تصل البيانات و إلى أين تتجه.

من أجل إنشاء شبكة اتصال خاصة مع مسار تور ، يقوم برنامج المستخدم ببناء دائرة اتصالات مشفرة تدريجيا من خلال تبديلات على الشبكة. يتم توسيع الدائرة بمعدل قفزة واحدة في كل مرة و كل تبديله تعلم من أي تبديله أخرى أتت البيانات و إلى أي تبديله ستتجه. و ليس باستطاعة أي تبديله معرفة المسار الكامل لحزمة البيانات أبدا. يقوم البرنامج الذي تستخدمه بمحاولة الحصول على مجموعة منفصلة من التشفير لكل قفزة على الدائرة من أجل ضمان عدم تتبع أي قفزة للاتصالات التي تجرى حاليا.

وبمجرد إنشاء دائرة ، يمكن تبادل أنواع كثيرة من البيانات ويمكن استخدام أنواع مختلفة من البرامج على شبكة تور. و لأن كل تبديله تعلم التبديلية اللاحقة و التبديلية التي سبقتها، لا يستطيع أي متنصت أو شخص يهدد الشبكة من استخدام تحليل حركة المرور لربط المستخدم بموقع معين أو وجهة معينة. تور يعمل فقط لدفقات تي سي بي و يمكن استخدامه مع أي تطبيق يدعم سوكس أي socks.

و لتحقيق الكفاءة ، برنامج تور يستخدم نفس الدائرة للاتصالات التي تحصل خلال فترة زمنها عشر دقائق تقريبا. أي طلبات لاحقة يتم الحاقها بدائرة جديدة ، لمنع الناس من ربط أفعالك السابقة بأفعال جديدة.

الخلط الرقمي

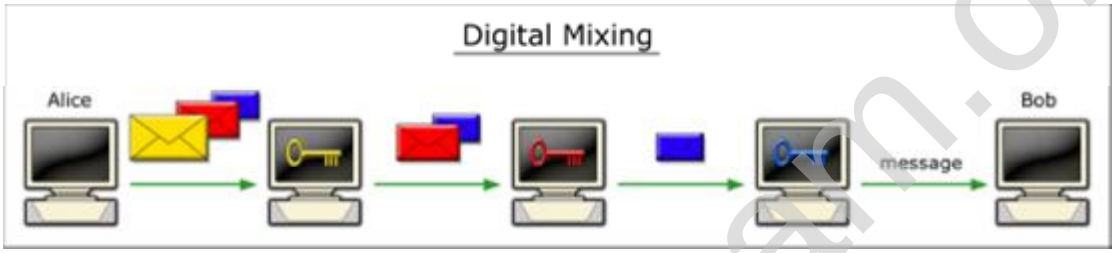
في أوائل الثمانينات من القرن الماضي، ابتكر ديفيد Chaum مبدأ يمزج الرقمية التي تسمى أحيانا شبكات مزيج لتحقيق مستوى أعلى من عدم الكشف عن هويته مع الاتصالات الشخصية . الخلط الرقمي يستخدم نظام مماثل لكنه يضيف توجيه عدة طبقات في الاتصال بين المرسل والمتلقي من التواصل .

$$Ciphertext = E_{PK1}[E_{PK2}[E_{PK3}[message]]]$$

الشكل 1 يوضح كيف يمكن لهذه الطبقات وظيفة في الممارسة العملية .يتم إنشاء الطبقات باستخدام التشفير بالمفتاح العمومي.

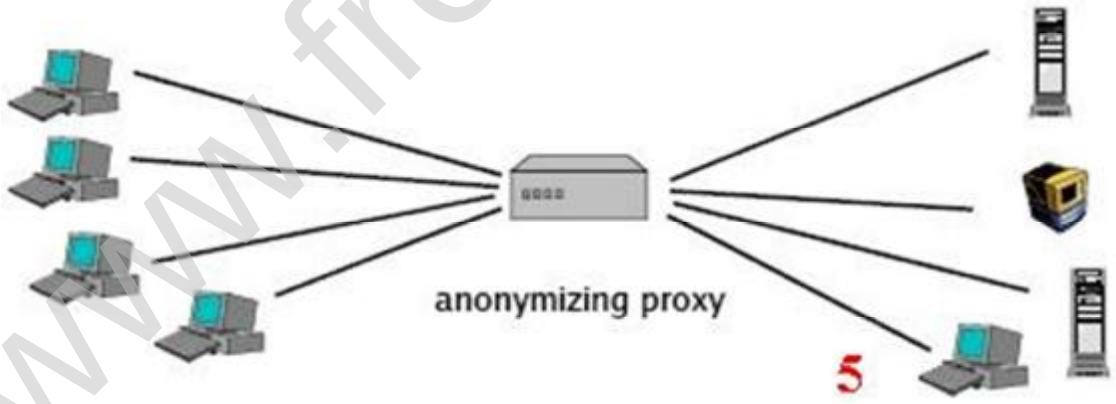
خلط الرسالة

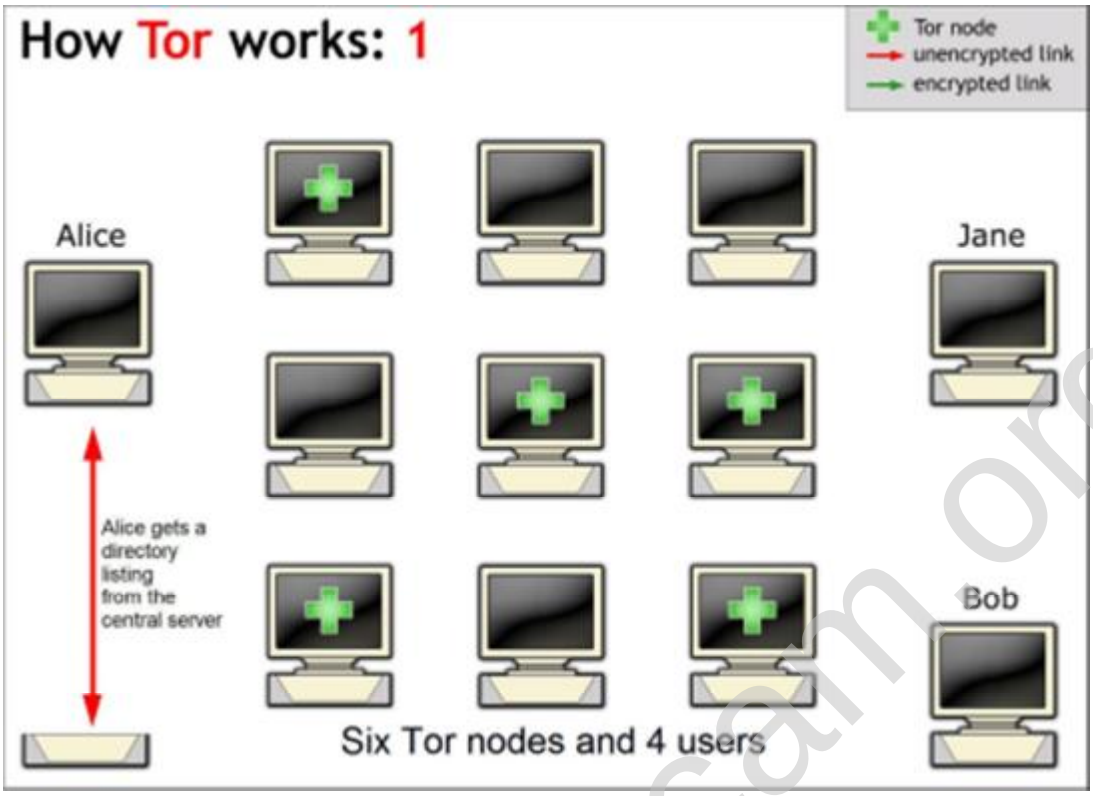
مثال اذا أراد محمد أن يبعث برسالة إلى سعد من دون ان يكون شخص ثالث على علم بمحتوى الرسالة وهواية المرسل او المتلقي
تور يقوم بتشفير الرسالة ثلاث مرات مع الدعم التشفير بالمفتاح العمومي .ثم يقوم بأرسالها الرسالة الملقم الوكيل الذي من شأنه أن يزيل الطبقة الأولى من التشفير وإرسالها إلى ملقم وكيل الثانية عن طريق استخدام التقليب .سيقوم هذا الملقم الثاني بفك التشفير، وارسال الرسالة الى الخادم الثالث الذى يقوم بفك تشفير الرسالة وإرسالها إلى المتلقي المقصود .ويتضح هذا في الشكل أدناه.

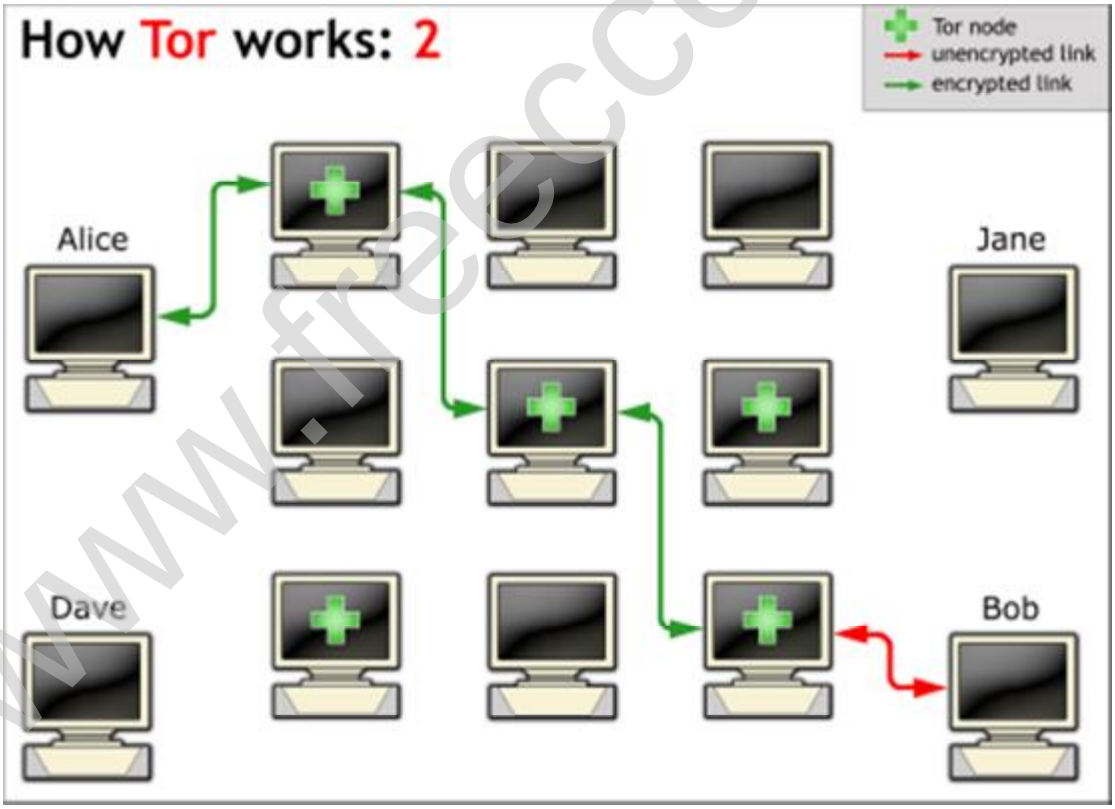


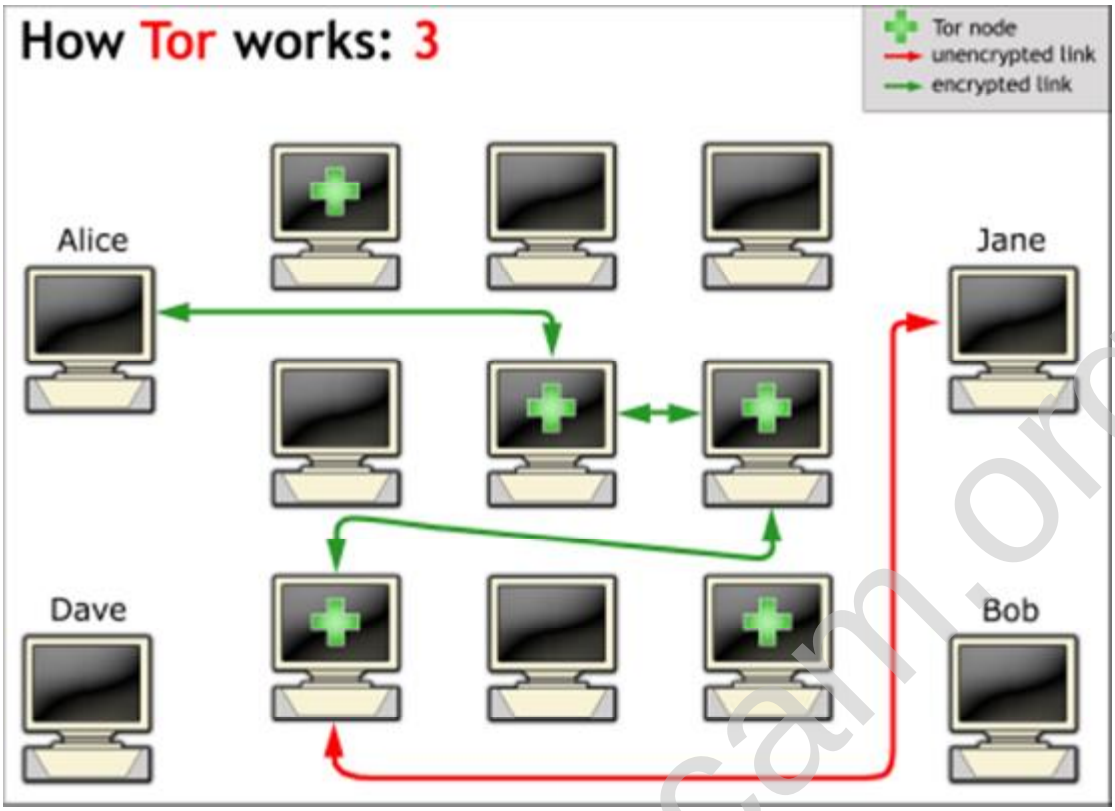
إخفاء الهوية الوكلاء

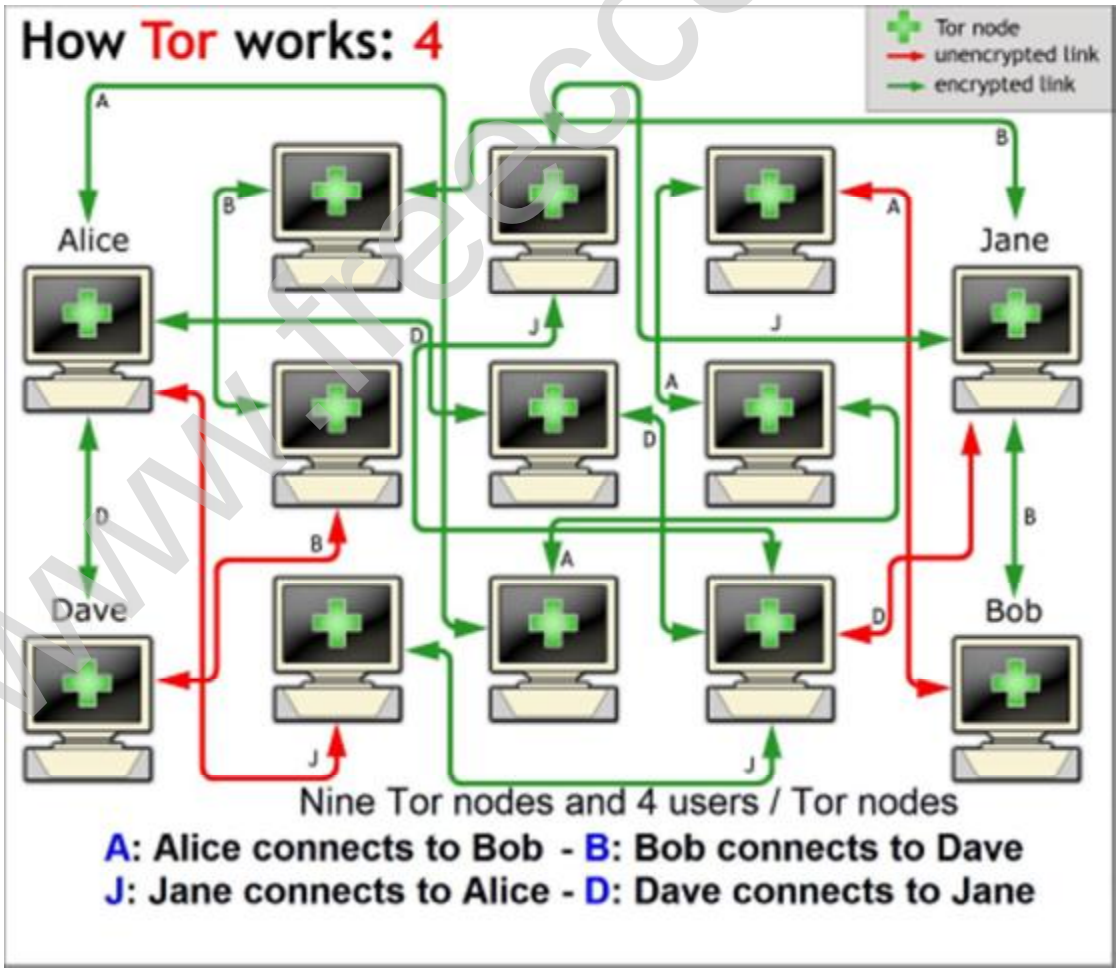
الملقم الوكيل يقوم بإخفاء الهوية وهو الخادم الذي يعمل فقط مع العقدة .هذا يعني أنه يطلب تعديل المسار فقط من موقع إلى آخر .محمد إذا أراد إجراء اتصال بسعد بدون علم الجهات الامنية فأن البرنامج يقوم بتغير عنوان IP محمد في ملقم الوكيل .والخادم الوكيل ثم إجراء اتصال مع سعد وتتابع كافة المعلومات الخاصة ويرسلها الى المتلقي











الخدمات المخفية

يمكن تور المستخدمين أيضا من إخفاء مواقعهم أثناء زيارة مواقع الانترنت أو خدمات التراسل الفوري أو الشات. باستخدام "نقاط لقاء" تور، يمكن للمستخدمين الآخرين استخدام هذه الخدمات المخفية من دون أن يعرف كل منهم هوية الشبكة الأخرى.

ويمكن لهذه الميزة أن تسمح للمستخدمين انشاء موقع على شبكة الانترنت حيث يستطيع الناس نشر مواد دون القلق بشأن الرقابة أو الحظر لن يكون أحد قادرا على تحديد من الذي قام بتوفير الموقع ، ولن يعلم موفر الموقع من قام بتحديثه أو نشر معلومات عليه.

البقاء مجهولا

ليس باستطاعة تور حل كافة مشاكل اخفاء الهوية . ويركز تور على حماية نقل البيانات فقط . تحتاج إلى استخدام البرمجيات الخاصة ببروتوكول الدعم إذا كنت لا ترغب في أن تقوم المواقع التي تزورها بمعرفة المعلومات الخاصة بك. على سبيل المثال ، يمكنك استخدام أثناء التصفح على شبكة الإنترنت منع الكوكيز وحجب المعلومات عن نوع المتصفح الخاص بك.

أيضا ، لحماية هويتك ، كن ذكيا. لا تذكر اسمك أو تكشف عن أي معلومات أخرى عند تعبئة نماذج أو طلبات على الانترنت. اعلم أن مثل جميع الشبكات التي تخفي الهوية و السريعة بالقدر الكافي لتصفح الإنترنت ، تور لا يوفر حماية ضد الهجمات التي تعتمد على توقيت الطرف الى الطرف الآخر : إذا تمكن المهاجم من مشاهدة حركة المرور القادمة من جهاز الكمبيوتر الخاص بك ، وكذلك حركة المرور في وجهتك، بإمكانه استخدام التحليل الإحصائي لاكتشاف أنهم جزء من الدائرة نفسها التي تقوم أنت باستخدامها..

مستقبل تور

يشكل توفير شبكة صالحة لإخفاء الهوية على شبكة الانترنت اليوم تحديا مستمرا. نريد برامجا تلبي احتياجات المستخدمين. كما نريد أيضا الحفاظ على الشبكة وتشغيلها بطريقة تسمح بخدمة أكبر عدد ممكن من المستخدمين. لا يجب أن يكون الأمن وسهولة الاستخدام أمرين متناقضين. كلما ازدادت صلاحية تور للاستخدام كلما زاد عدد المستخدمين مما يزيد من عدد المصادر و الوجهات المحتملة لكل عملية اتصال، و هذا في نهاية الأمر يزيد من أمن الجميع.

البداية

تم تصميم و تطبيق و نشر تور أصلا بوصفه الجيل الثالث من مشروع أونيون لتوجيه الاتصالات الخاص بمختبر بحوث البحرية .
وقد تم تصميمه مع اخذ البحرية الامريكية في عين الاعتبار ، و لغرض حماية الاتصالات الحكومية. اليوم ، يستخدم تور كل يوم للعديد من الأمور من قبل الصحفيين والعسكريين وموظفي اجهزة الامن ، والناشطين ، وكثير غيرهم. ما يلي بعض من الاستخدامات التي رأيناها أو نرتأها أي واحد منا

يستخدم الناس العاديون تور

يستخدم الناس العاديون تور لحماية خصوصياتهم من انظمة التسويق المتطفلة، منتحلي الشخصية ومزودي خدمة الانترنت الذين قد يبيعون سجلات التصفح للمسوقين أو أي شخص آخر على استعداد لدفع ثمنها.
مقدمي خدمات الإنترنت يقولون عادة أنهم يخفون البيانات من خلال عدم تقديم معلومات عن اشخاص محددين ، ولكن ثبت أن هذا غير صحيح و .

يمكن أن تحوي هذه البيانات على سجل كامل لكل موقع تزوره ، ونص كل بحث تقوم به، وحتى في بعض الاحيان اسم المستخدم وكلمة السر الخاصتين بك.

بالإضافة إلى موفري خدمة الإنترنت ، قد تحتوي المواقع التي تزورها ومحركات البحث على سجلات لنفس المعلومات أو اكثر.

يحمي هؤلاء الأشخاص اتصالاتهم من الشركات الغير مسؤولة في كل أنحاء شبكة الإنترنت ، يوصى باستخدام تور لكل الأشخاص الذين يخشون اي تهديد لخصوصيتهم من انتهاكات وخيانات قد تعرض معلوماتهم الحساسة للخطر .

في غالب الأحيان المعلومات التي قد تقوم بنشرها - مثل فيديو او صورة على فلاش ديسك أو جهاز هاتف نقال او حتى اقراص نسخ ، غالبا ما تكون غير محمية بشكل جيد من قبل أولئك الاشخاص او المؤسسات التي من المفترض أن تحميها.

انهم حماية الأطفال على الانترنت. يقوم مستخدمي تور ايضا بحماية أفراد عائلتهم بينما يكونون على الانترنت. **كيف** ؟ربما قد تكون نبهت أولادك الى عدم قول معلومات قد تعرفك شخصيا بينما هم يقومون بالشات او التحدث مع أصدقاء على فيسبوك لكنهم رغم ذلك قد يعطون معلومات عن اماكن وجودهم بدون أن يدروا من خلال عنوان الاي بي الخاص بجهاز الكمبيوتر.

وبصورة متزايدة، من الممكن هذه الايام الحصول على عنوان منزلك والحي والشارع من عنوان الاي بي الخاص بك.

عنوان الاي بي ايضا يقوم بتوفير معلومات اضافية عن كيفية استخدامك للإنترنت، و أي مواقع تزور وفي الولايات المتحدة ، تسعى الحكومة لجعل تحديد عنوان المنزل من عنوان الاي بي عملية اكثر دقة.

تشمل مواضيع حساسة ، يقوم مستخدمو تور أيضا بالقيام ببحوث . هناك ثروة من المعلومات المتاحة على الانترنت ولكن في بلدك ، قد تكون مواقع المعارضة الاخبارية او منظمات حقوق الانسان محجوبة خلف جدار

الجيش و قوات الحفاظ على النظام

تستخدم الجيوش و جماعات المعارضة تور أيضا

الأفراد في أرض الميدان: ليس من الصعب على المتمردين أو اجهزة المخابرات او الامن الداخلي مراقبة حركة الانترنت واكتشاف - مثلا - كل الفنادق والأماكن الأخرى التي يقوم البعض بالاتصال منها بسيرفرات محطة القيادة أو غرفة العمليات .

كما يقوم الافراد المنتشرون في أرض الميدان باستخدام تور لإخفاء المواقع التي يزورونها ، وحماية المصالح العسكرية والعمليات ، فضلا عن حماية أنفسهم من الأذى الجسدي.

الخدمات المخفية : عندما قامت مؤسسة داربا بتصميم الانترنت، كان غرضها الأساسي هو تسهيل القيام باتصالات موزعة و قوية في حالة وقوع اضرابات. ومع ذلك ، يجب أن تكون بعض المهام مركزية، مثل مواقع القيادة والسيطرة. الكشف عن الموقع الجغرافي لأي سيرفر هي من طبيعة بروتوكولات الإنترنت و هذا يشمل أي سيرفر موجود على الانترنت.

ولمنع هذا، تقوم خدمات تور المخفية بالسماح لعمليات لقيادة و السيطرة العسكرية ان تجرى بأمان و ان تكون فعلا محصنة من الاكتشاف و التعطيل.

جمع المعلومات الاستخبارية : يحتاج اعضاء القوات المسلحة الى استخدام المواقع التي تستخدمها الجماعات المتمردة و المسلحة. لكنهم في نفس الوقت لا يريدون لسجلات سيرفر الويب ان تبقى على موقع الجماعات تلك، كاشفة بذلك عناوين الاي بي العسكرية.

الصحفيون ووسائل الإعلام

يستخدم تور الصحفيون و جمهور القراء او المشاهدين
منظمة مراسلون بلا حدود تقوم بمتابعة سجناء الضمير الناشطون على الانترنت و ان كانوا محتجزين او قد تعرضوا لأي اذى في جميع أنحاء العالم. تقوم صحفيون بلا حدود بتوفير النصيحة للصحفيين و مصادر المعلومات، والمدونين ، و نشطاء المعارضة لاستخدام تور لضمان الخصوصية والأمان.

في الولايات المتحدة مكتب البث الدولي (صوت أمريكا \إذاعة أوروبا الحرة \ راديو آسيا الحرة) يدعم تطوير تور لمساعدة مستخدمي الإنترنت في البلدان التي لا يمكن استقبال وسائل الإعلام الحرة.
تور يحافظ على قدرة الأشخاص الموجودون وراء جدران الانترنت أو تحت المراقبة من الأنظمة القمعية الحصول على نظرة عالمية حول مواضيع مثيرة للجدل بما في ذلك الاقتصاد ، والديمقراطية والدين.

الصحفيون و المدونون في الصين يستخدمون تور للكتابة عن الأحداث المحلية لتشجيع التغيير الاجتماعي والإصلاح السياسي.

يقوم المواطنون والصحافيون في ثقوب الانترنت السوداء باستخدام تور لا جراء ابحاث عن الدعاية المغرضة الرسمية و وجهات النظر المعارضة ، و أيضا يقومون بإرسال مقالات صحفية لوسائل اعلام مستقلة و غير خاضعة للرقابة، من اجل تفادي العواقب الشخصية الخطرة على الفضول الفكري.

يستخدم ضباط اجهزة المخابرات والامن نظام تور

● **مراقبة الانترنت :** تور يسمح لمسؤولي المواقع على شبكة الإنترنت تصفح المواقع دون ترك آثار تدل عليهم . إذا كان المسؤول عن موقع اجرامي يرى وجود زيارة لموقعه من قبل مواقع حكومية او اجهزة أمن فان هذا قد يعيق التحقيقات.

● **العمليات السرية :** وبالمثل ، عدم الكشف عن الهوية يسمح لضباط الامن بالانخراط في "عمليات" سرية على الانترنت. بغض النظر عما ان كان الضابط جيدا في الميدان، فقد يتعرض غطائه للكشف ان كان هناك عناوين اي بي تنبع من نطاق سيرفرات الشرطة في الاتصالات التي يقوم بها.

● **تلميحات عن مواقع خدمات المعلومات الآمنة :** في حين تحظى مواقع و خطوط الهاتف المجانية للمعلومات بشعبية، الا انها أبعد ما تكون اكثر فائدة دون برنامج منفصل لإخفاء الهوية. المصادر المتطورة تفهم أنه على الرغم من ان من الممكن ان لا يحتوي عنوان البريد الإلكتروني أو اسم على أي معلومات الا ان سجلات السيرفر يمكن التعرف عليها بشكل سريع جدا. ونتيجة لذلك ، ومواقع التي تقوم بإخذ المعلومات بصيغة آمنة و التي لا تشجع على عدم الكشف عن الهوية تقوم اصلا بعدم توفير الحماية و السرية لمصادر المعلومات .

النشطاء و كاشفي الأسرار

● يستخدم نشطاء حقوق الإنسان تور لإرسال تقارير من دون كشف هويتهم عن الانتهاكات في المناطق الخطرة. وعلى الصعيد الدولي ، يستخدم النقابيون تور وغيرها من أشكال عدم الكشف عن الهوية حاليا لتنظيم العمال وفقا للإعلان العالمي لحقوق الإنسان. على الرغم من أن هذه الانشطة لا تنتهك القانون ، الا ان هذا لا يعني أنها آمنة. تور يوفر القدرة على تجنب الاضطهاد عندما ترفع صوتك و تجهر بالحقيقة.

- عندما تكون بعض الجماعات مثل لجنة خدمة الاصدقاء والجماعات البيئية الوقوع تحت المراقبة بالتعرض للمراقبة في الولايات المتحدة بموجب قوانين تهدف الى حماية مكافحة الإرهاب ، العديد من نشطاء التغيير السلمي يعتمدون على تور للحصول على خصوصية اثناء قيامهم بأنشطة مشروعة.

- هيومن رايتس ووتش توصي في تقريرها" السباق إلى القاع : تواطؤ الشركات في الرقابة على شبكة الإنترنت في الصين "، و قد قام كاتب هذا التقرير بإجراء مقابلة مع روجر دنغلدين ، رئيس مشروع تور، حول كيفية استخدام تور في اختراق "سور الحماية العظيم في الصين" ، ويوصي بأن العاملين في حقوق الإنسان في جميع أنحاء العالم يستخدمون تور "في التصفح الآمن والاتصالات."

- وقد تشاورت مع تور وتطوع لمساعدة منظمة العفو الدولية في الآونة الأخيرة حملة مسؤولية الشركات .

- الأصوات العالمية توصي تور ، وخاصة بالنسبة المدونات المجهول ، في جميع أنحاء بهم موقع ويب.

- في الولايات المتحدة ، وجردت المحكمة العليا مؤخرا الحماية القانونية من المخبرين الحكومة. ولكن يمكن أن المخبرين العمل من أجل الشفافية الحكومية أو مساءلة الشركات استخدام تور لتحقيق العدالة من دون تداعيات الشخصية.

- يمكن تور مساعدة الناشطين تجنب الرقابة الحكومية أو الشركات التي تحول دون تنظيم. في حالة واحدة من هذا القبيل ، و منعت الوصول إلى خدمة الإنترنت الكندية موقع على شبكة الانترنت التي يستخدمها الاتحاد الخاصة موظفيها للمساعدة في تنظيم الإضراب.

مدراء الشركات يستخدمون تور

- **تجميع معلومات الاختراقات الأمنية:** تخيل أن منظمة اقتصادية ما مشتركة في جمع معلومات عن اختراقات الإنترنت في مخزن للبيانات.
سوف يحتاج الأعضاء المشتركون إلى إبلاغ مجموعة معينة مركزية عن الاختراقات لتقوم بالبحث عن أسبابها لاكتشاف العامل المشترك وإرسال التحذيرات للبنوك الأخرى. لو تم اختراق بنك معين فلن يرغب طاقمه بأن يعرف أي مهاجم يراقب المخزن بذلك؛ وعلى الرغم من أن كل الحزم معماه إلا أن عنوان IP سوف يكشف مكان النظام المخترق.

- **الحفاظ على سرية الاستراتيجيات و الخطط:** على سبيل المثال، قد لا تريد من المتلصصون الصناعيين يكون قادرين على تتبع ما مواقع ويب المحللين للأهمية الاستراتيجية لأنماط حركة المرور ، وضعف الرقابة على مثل هذه البيانات ، هو بداية لتكون أكثر المعترف بها على نطاق واسع في مجالات عدة في عالم الأعمال.

- **المسائلة :** في عالمنا حيث تقوم الانشطة التجارية الغير معروفة بتقويض شركات فيمتها تبلغ مليارات الدولارات، من الممكن للمسؤول التنفيذي ممارسة دوره في تعزيز الثقة في شركته

بحيث يشعر الجميع بقدرتهم على الحديث عن عمليات التخريب الداخلية. يساعد تور على تحقيق المسائلة الداخلية في الشركات لكي لا تصبح سرا قد يتم كشفه للإعلام و المنافسين

يستخدم المدونون تور

نسمع دائمًا عن مقاضاة المدونين أو طردهم لمجرد أنهم تحدثوا بقانونية تامة على الإنترنت في مدوناتهم.

- ننصح بدليل مؤسسة الجبهة الإلكترونية القانوني للمدونين.
- ترعى Global Voices دليلا عن التدوين السري باستخدام وورد برس وتور.

خبراء التقنية يستخدمون تور

★ للتأكد من إعدادات الجدر النارية حيث يمكن أن تسمح سياسات بعض الجدر النارية لعناوين أو نطاقات IP معينة فقط. يمكن أن يستخدم تور للتأكد من هذه الإعدادات عبر استخدام رقم IP من خارج نطاق عناوين IP التابعة الشركة.

★ **لتجاوز أنظمتهم الأمنية لنشاطات مهنية حساسة:** يمكن أن تُقيّد شركة ما المواد التي يمكن لموظفيها مشاهدتها على الإنترنت.
إذا وُجد خرق محتمل لتلك السياسة في السجل، يمكن أن يُستخدم تور للتأكد من المعلومات دون التسبب في تسجيل تحذير في أنظمة الشركة الأمنية.

★ **للاتصال بالخدمات المنشورة:** يمكن لمهندس شبكة أن يستخدم تور للاتصال بالخدمات التي يشغلها دون الحاجة إلى جهاز خارجي وحساب مستخدم. يتم ذلك عادة لغرض الاختبار.

★ **للوصول إلى موارد الإنترنت:** تختلف عادة سياسات السماح باستخدام الإنترنت بين الطاقم التقني والموظفين العاديين. يمكن أن يستخدم تور للوصول غير المقيد للإنترنت مع ترك سياسات الأمن دون تغيير.

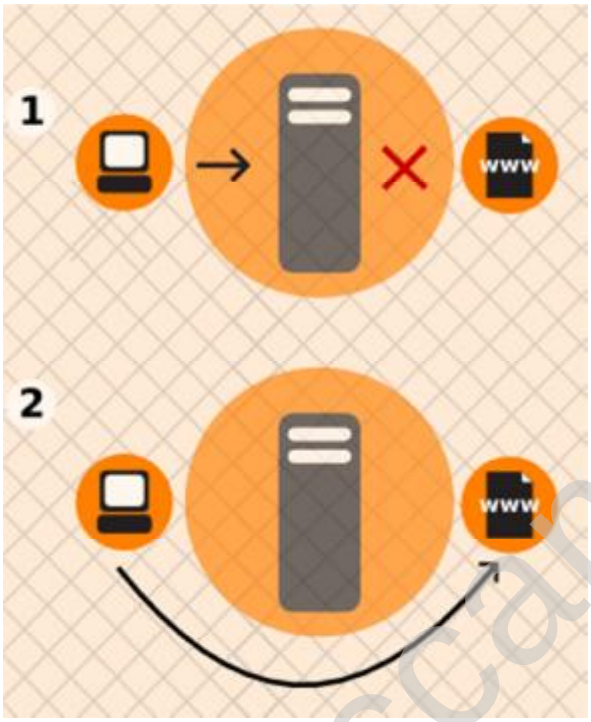
★ **لمعالجة مشاكل شبكة مزود الإنترنت:** يمكن أن يجعل تور محتويات الإنترنت متوفرة في الأوقات التي يواجه فيها مزود الإنترنت مشاكل في التوجيه أو في DNS. قد لا يقدر هذا بثمن في الحالات الطارئة.

مثل كل التقنيات من أقلام الرصاص إلى الهواتف النقالة، يمكن أن تستخدم السرية لأغراض جيدة وسيئة.
ربما شاهدت مختلف النقاشات (المؤيدة والمعارضة والأكاديمية) عن السرية. إن مشروع تور مبني على الاعتقاد أن السرية ليست جيدة فحسب، بل ضرورة لحرية المجتمع وسيره.
تشرف مؤسسة الجبهة الإلكترونية (EFF) على ملخص جيد لدور السرية الأساسي في تأسيس الولايات المتحدة. لقد أقرت المحاكم السرية حقًا أساسيًا وهامًا.
في الحقيقة الحكومات تلتزم بالسرية في أحوال كثيرة مثل: البلاغات الأمنية وخدمات التبني وهويات ضباط الشرطة وغيرها.
من الصعوبة بمكان سرد مناقشة السرية بالكامل هنا لأنها قضية كبيرة جدًا ولها ظلال كثيرة وتوجد أماكن أخرى عديدة يمكن أن تجد تلك المناقشات فيها.

تجاوز الحجب على الإنترنت

توجد عدد من الطرق لتجاوز الحجب على الإنترنت، تشمل أدوات برمجية و مسارات محمية، و يشار إلى تلك الأساليب في مجملها بأنها أساليب تجاوز الحجب و هي تتراوح ما بين الالتفافات البسيطة و البرمجيات الحاسوبية المعقدة. فمثلا، أحيانا تمكن مطالعة موقع محجوب

بمجرد طلب نسخة مخبئة من صفحاته يكون قد حفظها محرك البحث، عوضا عن السعي إلى زيارة الموقع المحجوب ذاته



مُيَسِّرو التجاوز

ميسرو التجاوز هم أفراد أو منظمات يقدمون تسهيلات لتجاوز الحجب و الرقابة على الإنترنت، و هم قد يكونون منظمات تجارية كبيرة تقدم خدمات تجاوز مقابل أجر، أو أفرادا أو منظمات تقدم خدمات التجاوز مجانا، و عادة ما يعمل ميسرو التجاوز على تنصيب برمجيات على حواسيب في مواضع لا حجب فيها ثم يتيحون للأخرين ممن يضطرون إلى الاتصال بالإنترنت من أماكن يُفرض عليهم فيها الحجب الاتصال بتلك الحواسيب كوسطاء بينهم و بين الإنترنت، عوضا عن الاتصال المباشر الذي يمكن من خلاله فرض الحجب عليهم.

مستخدمو التجاوز

مستخدمو التجاوز هم أفراد أو منظمات يستخدمون تقنيات التجاوز في المواضع التي يلجون منها إلى الإنترنت بهدف النفاذ إلى محتوى محجوب أو إرسال معلومات من مواضع تحظر ذلك، سواء كان القائم بالحظر و الرقابة هو صاحب العمل أو جهة أمنية مخابراتية أو رقيبا حكوميا

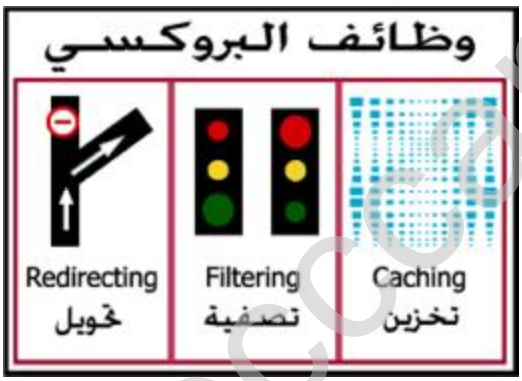
مهم قبل ان نبداء شرح البرنامج يجب ان نوضح الفرق بين التّور وبرامج البروكسي الأخرى

ما هو البروكسي؟

البروكسي هو برنامج (Software) يتم تركيبه على أجهزة خادمة. و لذلك يسمّى مجازاً باسم: خادم البروكسي. مثله في ذلك مثل خادم الويب. الذي هو أيضاً عبارة عن خادم برمجي.

ماهي وظائف البروكسي

وظائف البروكسي هي كما ترى في الصورة ادناه ، تجد أن للبروكسي ثلاث وظائف رئيسية:



1 التخزين (**Caching**): و هذه الوظيفة الأساسية للبروكسي. بحيث يقوم بتخزين المواقع والصفحات، حسب ما تم تخصيصه عليه، و تقديمها للمستخدم. و هذا من شأنه أن يجعل التصفح أسرع.

2 التصفية (**Filtering**): و هذه العملية يقوم بها البروكسي بشكل جانبي بالإضافة للعملية الأساسية و هي الـ caching. بحيث يقوم بحجز المواقع غير المرغوبة، و السماح لغيرها من الطلبات بالمرور. و من الجدير بالذكر أن البروكسي لا يقوم بذلك بشكل أساسي، بينما يقوم برنامج من نوع **Firewall** بذلك بكفاءة أكبر.

3 التحويل (**Redirection**): و هو أن يقوم بتحويل بعض طلبات المواقع إلى جهات أخرى. كأن يقوم بتحويل طلبات المواقع غير اللائقة إلى موقع اسلام واي مثلاً..

ما الفائدة من التخزين؟

ان عملية تخزين المعلومات في الخادم الذي تم تركيب البروكسي عليه، تجعل الانترنت سريعة. ستسألني: كيف؟

لنتخيل معاً أن انك حينما تطلب صفحة من الانترنت، فإن هناك عاملاً في الشبكات، يطوف الانترنت بحثاً عن هذا الموقع، حتى يجده، ثم يقوم بنقله لك، و هو حين ينقله، يقوم بنقل الصفحة كنص أولاً، ثم ينطلق مرة اخرى، ليذهب إلى الموقع ليجلب الصورة الأولى في الموقع، و عندما يحضرها لك، ينطلق مرة أخرى، و هكذا حتى تنتهي جميع مكونات الصفحة من صور و فيديو و نص. لننظر للصورة:

و لكن لنتخيل أنه يوجد شخص لديه آلة تصوير فوتوغرافية عندما يتم طلب الموقع أول مرة، يذهب صاحبنا المسكين ليجلب مكونات الموقع من الخادم الذي قد يكون موجوداً في دولة أخرى. و عندها يقوم صاحب آلة التصوير الموجود في نفس بلدك بنسخ جميع مكونات الموقع و يحفظه لديه، و يكتب عليه التاريخ، و عندما يقوم مستخدم آخر بطلب نفس الموقع، فإن العامل المسؤول

عن جلب الموقع، يقوم بإحضاره من صاحب آلة التصوير القريب، و لا يذهب للموقع عبر دهاليز الانترنت. و هذا يجعل الانترنت أسرع.

من المفيد هنا أن نذكر بعض المميزات التي يتمتع بها خادم البروكسي (و التي قد تختلف من شركة لأخرى)، مثل امكانية تخصيصه بحيث يقوم بتحديث المواقع التي تتحدث بشكل سريع مثل المواقع الاخبارية او المواقع النشطة الأخرى أثناء الليل. فكون البروكسي موجود في نفس البلد يقوم باستغلال الفترة الميتة التي تكون الانترنت فيها غير نشطة بشكل كبير، و يقوم بتحديث المواقع، و هذا يجعلها تكون جديدة دائماً عندما يطلبها المستخدم.

لاحظ أنك حين تضغط على زر التحديث **(Reload - Refresh)** في المتصفح، يقوم بتحديث الصفحة من الموقع الأصلي، و هذا يجعل عملية التحديث تأخذ وقتاً أطول نسبياً من عملية الطلب.

كذلك لاحظ أنك حين تقوم بزيارة احدى الصفحات والتي يتصادف كونك الزائر الأول لها، سيقوم البروكسي بجلب الصفحة و نسخها، و هذا قد يجعل المسألة تأخذ وقتاً أطول نسبياً من المعتاد.

-

ما هو البروكسي اذن؟

تحذير **البروكسي هو وسلية لكسر الحجب لا غير**. ولو اتاح لك خدمة تشفير المعلومات , فهو دائما يمتلك المعلومات الوافية عليك وبإمكانه ايضا دس ما يشاء في المعلومات المتبادلة.

بإمكان نقاط التنصت والتجسس مراقبة مثلا مداخل المواقع المحجوبة والفيس بوك والمواقع الاخرى ومراقبة الاتصالات بالخادم الحاضن لتلك المواقع" ثم يقوموا بعملية عودة عكسية ليكتشفوا ان المتصل هو بروكسي وطبعا البروكسي لن يتردد لحظة واحد في اعطاء المخابرات الغربية والجهات الامنية ما تحتاجه " لا تغرنك اكاذيب حقوق الانسان وغيرها من الخزعبلات..." فالكفر اليوم اجتمع علينا واغلب البر وكسيات امريكية...

من ناحية أخرى **المعلومات بيننا وبين البروكسي غير مشفرة** اغلب الاحيان مما يمكّن السلطات التي تتابع الانترانت من الكشف على تلك المعلومات وبالتالي معرفة اننا نتصل بالمواقع الممنوعة الوصول اليها من قبل سلطات بلدك عندها سوف تجد نفسك فى احدى سجون بشار وسجون الفرس المجوس

التخفي في تصفح الانترنت وهذا هو موضوعنا الاساسي عن طريق برنامج تور الذى سوف نقوم بشرحه بالتفصيل ان شاء ألله ونبين كيف يمكنك التخفي وبعض الطرق او المعلومات العامة التي تفيد في التخفي في التصفح على الشبكة

أخواني أخواتي الاعزاء في سوريا الحبيبة والاهواز المحتلة نقول لكم الان انه يمكن الاعتماد على هذا البرنامج في حالة ضبط اعداداته الضبط الصحيح والتعامل معه حسب الشرح المصور عندها ان شاء الله يكون لا خوف عليكم من زبانية بشار وعصابته ولا خوف على اهل الاهواز من المحتل اللعين الفارسي المجوسي الذى يرقب كل تحركات من في الاحواز مع الاحتياط الشديد واخذ الحيطة والحذر المعتادة بارك الله فيكم

هل أنا مُراقَب أو يُحجبُ عني محتوى؟

لا يخفى أن حكومات دول عدة تمارس رقابة على محتوى الإنترنت، كما هو موثق في دراسات و كتب عديدة، منها دراسات أنجزتها مبادرة الإنترنت المنفتح و مركز بركمان في جامعة هارفارد و دراسة الشبكة العربية لمعلومات حقوق الإنسان المعنونة "خصم عنيد: الإنترنت و الحكومات العربية" التي تتناول حالة الحجب في الدول العربية، فعندما يُحجب موقع شهير فإن خبر هذا الحجب يذيع في البلد.

لكن عموما أحيانا ما يَصعُب التيقن مما إن كان أحدهم يحول دونك و الوصول إلى موقع وِب او من إرسال معلومات إلى آخرين. فعندما تحاول النفاذ إلى موقع محجوب قد تظهر لك رسالة عُطل معتادة تبلغك أن الموقع قد تعذَّر النفاذ إليه، و يمكن ألا يظهر شيء على الإطلاق، و هو ما قد يبدو معه أن الموقع غير متاح لأسباب تقنية.

بعض المنظمات مثل مبادرة الإنترنت المنفتحة (http://opennet.net) تستخدم برمجيات لاختبار نفاذية الإنترنت في دول مختلفة و لفهم الكيفية التي يمكن أن يؤثر بها الأطراف المختلفون على ذلك. في بعض الحالات يكون ذلك عسيرا أو حتى خطيرا، حسب طبيعة السُّلطة المعنية.

المراقبة و المجهولية

الأدوات المستخدمة لتجاوز كل من الحجب و الترشيح و المراقبة على الإنترنت مصممة لمعالجة مشكلات و عقبات مختلفة، فهذه الأدوات يمكن أن تعين على زيادة القدرة على النفاذ إلى المعلومات و الاتصال بالناس، و تفادي المخاطر المتعلقة بذاك النفاذ. فالأدوات المختلفة يمكن أن تُيسر:

- تجاوز الحجب: مطالعة أو نشر الوثائق أو أنواع أخرى من المحتوى على الإنترنت، و إرسال أو تلقي المعلومات، و الاتصال بناس آخرين أو بمواقع و خدمات بتجاوز محاولة منع ذلك التواصل. مثلا، مطالعة صفحة من مخبئة جوجل أو من مجمع تلقيمات (أتوم أو آرإس‌إس) بدلا من الموقع الاصلي ذاته.

- منع التنصت: الحفاظ على سرية الاتصالات بحيث لا يمكن لغير المعني بالاتصال مطالعة فحواه (لكن مع هذا قد يكون بوسعهم معرفة بمن تتصل) الأدوات التي تهدف إلى تجاوز الحجب دون منع التنصت يمكن أن استخدامها عرضة للرقابة و الحجب بطريق الترشيح بالكلمات المفتاحية و هو أسلوب يحجب كل الاتصالات التي تحوى كلمات معينة محظورة. مثلا، يمكن باستخدام أنواع عدة من التعمية تأمين بروتوكولات الاتصال مثل https أو ssh لتأمين قناة الاتصال ضد التنصت على المحتوى المار فيها لأي شخص غير طرفي الاتصال المعنيين.

- الحفاظ على المجهولية: القدرة على التواصل بحيث لا يمكن الربط بينك و بين المعلومات أو الأشخاص التي تتواصل بهم - قد يكون من يقصد الحفاظ على المجهولية في مواجهته هو مقدم خدمة الإنترنت، أو الموقع الذي تطالعه او الشخص الذي تتواصل معه، أو كليهما. مثلا مرسلات البريد المُجهِّلة و بعض خدمات الوسطاء مثل شبكة تور (عند اتخاذ احتياطات خاصة للمجهولية) يمكن أن تحقق هذا الغرض.

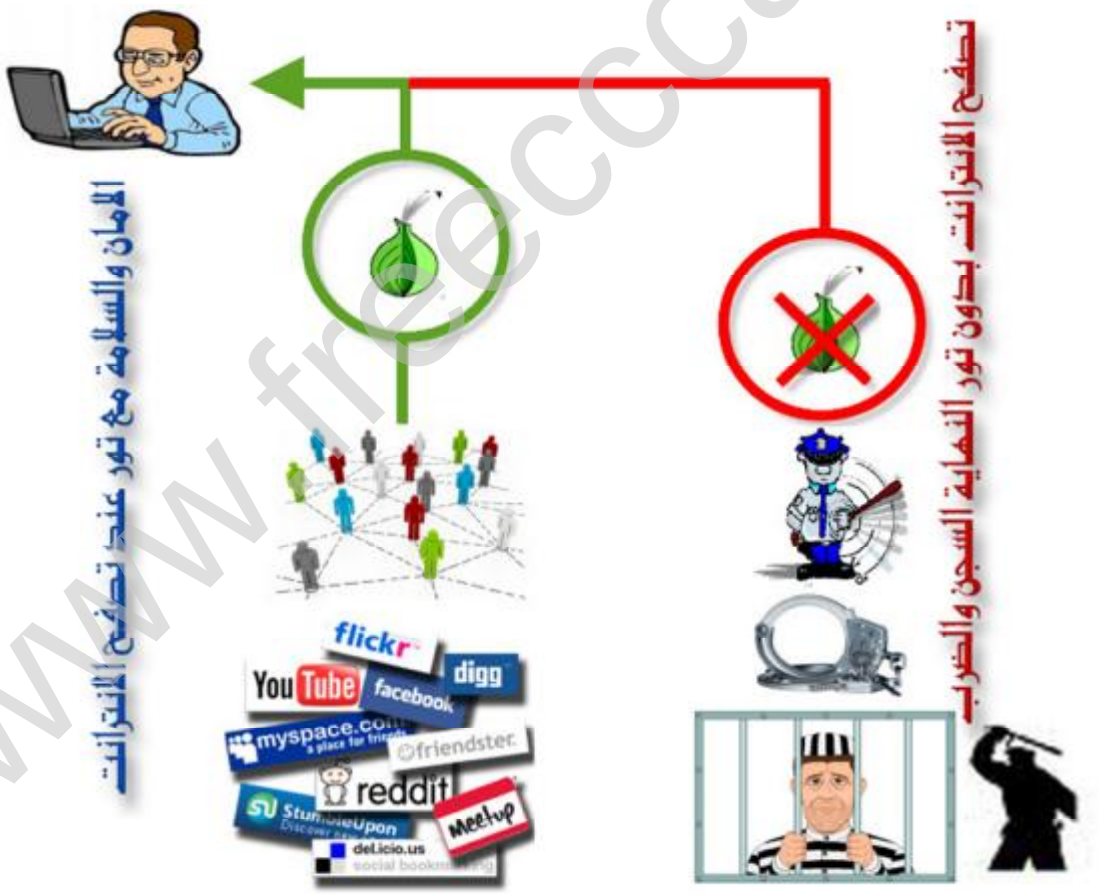
- إخفاء ما تقوم به: تمويه الاتصال الذي تقوم به بحيث لا تمكن للمراقب معرفة أنك تسعى لتجاوز الرقابة. مثلا، تقنيات الاستگانوغرافيا تعمل على إخفاء الرسالة - قد تكون نصية - في حاوية خارجية غير هامة - قد تكون صورة مثلا.

بعض الأدوات تحمي اتصالك في واحد من المجالات السالفة و حسب. فمثلا، كثير من الخواديم الوسيطة يمكن أن تعين على تجاوز الحجب لكنها لا تمنع التنصت، أي أنها تمكن المستخدم من

مطالعة موقع محجوب إلا أنها لا تمنع شخصا أو جهة من مراقبة ما تطالعه من المهم إدراك الحاجة إلى توليفة من الأدوات لتحقيق الأغراض المطلوبة كلها.

كل نوع من الحماية يهم أشخاصا مختلفين في ظروف مختلفة. فعند استخدام أدوات تجاوز حجب الإنترنت ينبغي أن نأخذ في الحسبان أي نوع من الحماية نريد و ما إذا كانت الأداة المستخدمة تحقق هذه الحماية. مثلا، ما الذي يمكن أن يحدث عندما تدرك الجهة الرقابية أنك تسعى إلى تجاوز الرقابة؟ و كذلك، هل يهمك إخفاء فحوى ما تطالعه أم أن ما يعنيك هو القدرة على مطالعته و حسب؟

أحيانا يمكن لأداة واحدة أن تستخدم لتحقيق أكثر من غرض، مثل تجاوز الرقابة و حماية المجهولية، غير أن تحقيق كل غرض قد يتطلب أسلوب استخدام مختلف. فمثلا يمكن باستخدام تور تحقيق كل من الغرضين، إلا أن مستخدمي تور المعنيين بأي من الهدفين أو بكليهما يستخدمونه بشكل مختلف.



تحذير هام

معظم أدوات تجاوز الرقابة و الحجب يمكن لمدير الشبكة أو الوكالات الحكومية تَحُّسس استخدامها، إذ أن تدفقات البيانات التي تولدها لها أنماط مميزة. هذا أكيد فيما يتعلق بأدوات التجاوز التي لا توظف التعمية، إلا أنه قد ينطبق كذلك على الأدوات التي توظف التعمية، و ذلك حسب تصميمها. كذلك تنبغي ملاحظة أنه حتى عند استخدام التعمية فقد يصعب إخفاء حقيقة استخدامها عن المراقب. عموما، من العسير الحفاظ على سرية حقيقة أنك تستخدم تقنيات التجاوز، خاصة إذا استخدمت تقنيات شائعة أو واظبت على استخدام الخدمة ذاتها لمدة طويلة. كما توجد أساليب لتحسس سلوكك لا تعتمد على التقنية: المراقبة الشخصية، و أساليب عديدة أخرى للتقصي و الاستدلال.

لا يمكن لهذا الدليل أن يقدم نصيحة محددة أو تقييما للمخاطر أو توصية بأدوات معينة لمواجهة مخاطر معينة، فالمخاطر تختلف باختلاف الظروف و هي تتغير طوال الوقت، و ينبغي أن تتوقع على الدوام أن من يسعون لتقييد نشاطك أو قدرتك على الاتصال و تلقي المعلومات سيطورون أساليبهم مع الوقت.

إن كنت تقوم بنشاط قد يعرضك للخطر فينبغي أن تحكم بنفسك عن درجة أمانك متسلحا بالمعرفة التي تتلقاها من هذا الدليل و ما يشبهه، و أن تستشير خبراء في المجال موثوقين إن كان ذلك ممكنا.

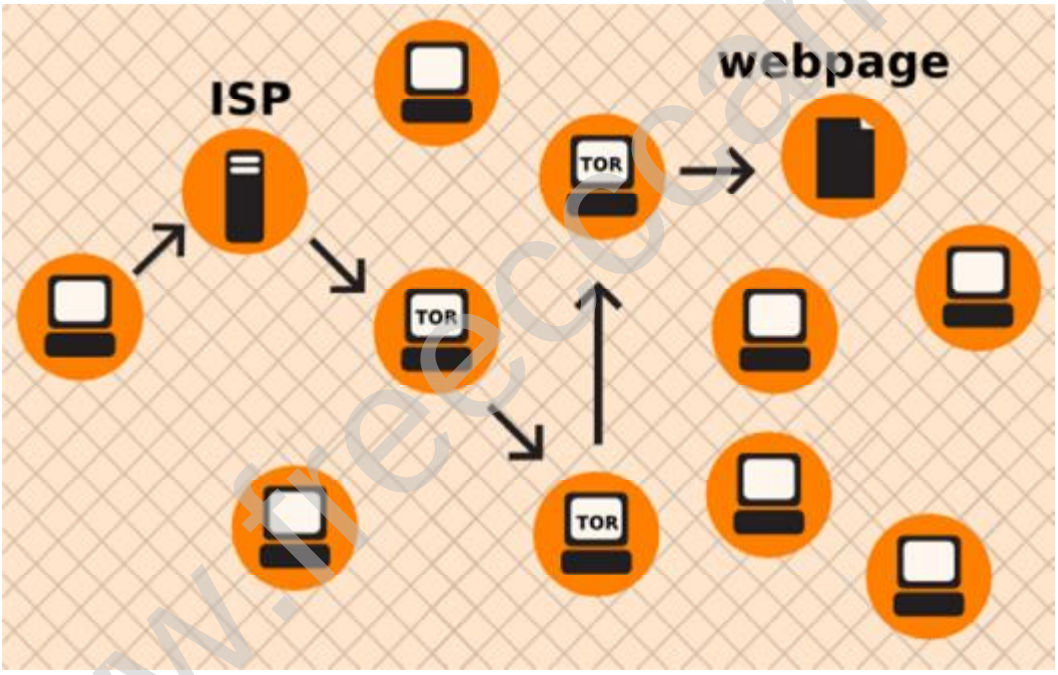
- إن اخترت وسيلة تتطلب الاعتماد على آخرين لا تعرفهم فاتخذ ما تراه من احتياطات و قيّم درجة ثقتك فيهم.
- تذكَّر أن وعود الحفاظ على المجهولية و الخصوصية التي تروجها الخدمات و البرمجيات المختلفة قد لا تكون دقيقة أو صحيحة. دوما استشر رأيَ محايدٍ.
- قد يتطلب الحفاظ على المجهولية و الخصوصية انضباطا ذاتيا و اتباعا صارما لإجراءات معينة و ممارسات عند العمل. التهاون في إجراءات السرية يقلل كثيرا من السرية و المجهولية، و قد يزيد أثره السلبي بسبب الإحساس الزائف بتحقق الأمان و الخصوصية.
- راع أنه يمكن لجهات و أشخاص عديدون، بمن فيهم الحكومات، نصب فخور العسل (HONEYPOTS) و هي مواقع وب و خدمات وهمية تتظاهر بتقديم اتصالات مؤمَّنة إلا أنها في الواقع تتلقى الاتصالات من المستخدمين غير الحذرين و تمررها إلى من يشغلها.
- انتبه للتهديدات غير التقنية، مثل ماذا يحدث إن سرق أحدهم حاسوبك أو هاتفك المحمول أو إن صودر منك؟ و ماذا يحدث إن نظر العامل في مقهى الإنترنت من فوق ظهرك؟ و ماذا يحدث إن جلس أحدهم ليستخدم حاسوبا في مقهى إنترنت كان صديق لك قد استخدمه قبله و نسي أن يقفل حسابه البريدي أو ينهي جلسة الدردشة؟

إن كانت التشريعات أو اللوائح التي تقيد أو تمنع المحتوى الذي تسعى للنفاذ إليه أو الأنشطة التي تمارسها فتمعن في التبعات المحتملة.

الحجب أو الرقابة يمكن كذلك أن يجريان لأسباب مختلفة غير متعلقة بالسياسة. فالآباء قد يرشحون المعلومات التي يمكن لأبنائهم النفاذ إليها، كما أن منظمات عدة، من المدارس إلى الشركات التجارية و المؤسسات الحكومية تُقيِّد النفاذ عبر الإنترنت لمنع مستخدميها من إجراء اتصالات غير مراقبة، باستغلال وقت أو موارد الشركة لأغراض شخصية، أو بانتهاك حقوق الملكية الفكرية، و أسباب أخرى

الموجه البصلة TOR

يعد Tor (الموجه البصلة) شبكة في غاية التعقيد من خوادم البروكسي.



عندما تستخدم Tor للوصول إلى موقع إلكتروني ما، يتم توجيه اتصالاتك بشكل عشوائي في شبكة من البر وكسيات المستقلة والتطوعية وكافة الحركات بين خوادم Tor (أو المرحلات) مشفرة، وكل من المرحلات يعرف فقط عنوان الـ IP الخاص بمرحلين آخرين -- المرحل الذي يسبقه فوراً في السلسلة وذلك الذي يليه.

وهذا الأمر يصعب:

على مزود خدمة الإنترنت (ISP) الخاص بك معرفة الموقع الإلكتروني الذي تقصده والمعلومات التي ترسلها على الموقع الإلكتروني المستهدف معرفة من أنت (أو على الأقل معرفة عنوان الـ IP الخاص بك) على أي من المرحلات المستقلة معرفة من أنت وإلى أين أنت ذاهب.

ما الذي تحتاج إليه لاستعمال شبكة Tor؟

للاتصال بالإنترنت من خلال شبكة **Tor** واستعمالها لأغراض المجهولية وتجاوز الحجب، ينبغي عليك تثبيت برنامج عميل **Tor** على حاسوبك. **(وبالإمكان أيضاً تشغيل نسخة محمولة من البرنامج من الفلاش ميموري ذاكرة أو أي أداة خارجية أخرى.)**

يعمل Tor مع معظم منصات التشغيل منها معظم إصدارات ويندوز وماك أو اي إكس ولينكس

ما البرامج التي ينسجم Tor معها؟

يستخدم Tor واجهة **SOCKS** بروكسي للاتصال بالتطبيقات، لذا يمكن جعل أي تطبيق يدعم **SOCKS** (الإصدارات 4 و 4a و5) مجهولاً باستخدام **TOR** بما في ذلك:

* معظم متصفحات الإنترنت
* العديد من برامج الرسائل الفورية وعملاء IRC
* عملاء SSH
* عملاء البريد الإلكتروني

قد يكون Tor أداة في غاية الفعالية لتجاوز الحجب ولحماية هويتك. فتشفير Tor يخفي محتويات اتصالاتك عن مشغل شبكتك المحلي، ويخفي هوية الأطراف التي تتصل بها أو المواقع التي تزورها. وعند استعماله بالشكل المناسب فهو يزودك بقدر أكبر وأقوى من حماية المجهولية من البروكسي المنفرد.

ولكن **Tor** عرضة للحجب. فمعظم عقد **Tor** مدرجة في قائمة عامة، لذا من السهل لمشغلي الشبكات الوصول إلى القائمة وإضافة عناوين الـ**IP** الخاصة بالعقد إلى الفلتر. (إحدى

الطرق لمحاولة تجاوز هذا النوع من الحجب هو استخدام أحد جسور بريدجات TOR العديدة التي هي عبارة عن عقد Tor غير مدرجة للعلن وذلك لتجنب الحجب بشكل خاص)

- بعض البرامج التي قد تستعملها مع Tor تعاني من مشاكل قد تعرض مجهوليتك للخطر.
- وإضافة لذلك، إذا لم تستخدم تشفيراً إضافياً لحماية اتصالاتك، فسيتم فك تشفير بياناتك فور وصولها إلى عقدة Tor الأخيرة في السلسلة (والتي تسمى بعقدة الخروج). وهذا يعني أنه من المحتمل أن تصبح بياناتك مرئية لمالك عقدة Tor الأخيرة ولمزود خدمة الإنترنت (ISP) بين تلك العقدة والموقع الإلكتروني الذي تقصده.

إن كنت مهتماً بشكل أكثر باستعمال Tor لتصفح الإنترنت والدردشة فقد يكون من الأسهل لك استعمال TOR BROWSER BUNDLE أو TOR IM BROWSER BUNDLE التي ستزودك بحلول جاهزة للاستعمال تم تشكيلها مسبقاً. وتشتمل كذلك مجموعة Tor للمتصفح على TORBUTTON الذي يعمل على تحسين حماية الخصوصية عند استعمال Tor مع متصفحات الإنترنت. ويمكن تنزيل كلا الإصدارين من الموقع الرسمي للبرنامج

الان بعون الله نبدأ في شرح برنامج تور و اول خطوة هي التوجه الى الموقع الرسمي للبرنامج من اجل تحميل البرنامج كما تشاهد في الشرح المصور

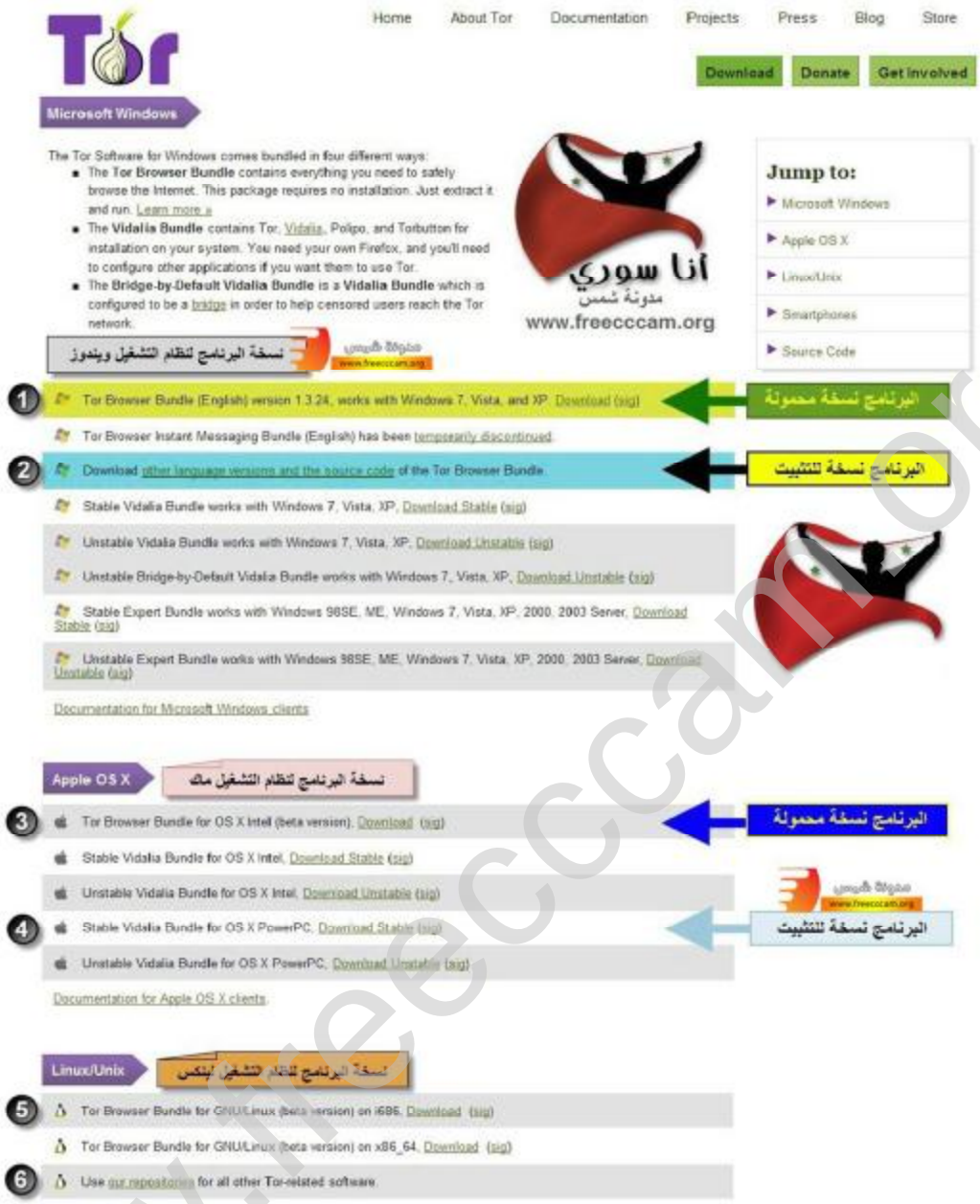
ملاحظة مهمة جدا وخطيرة

لا تقم بتحميل برنامج تور من أي موقع فقط عليك تنزيل البرنامج من موقعه الرسمي فقط وذلك تفاديا من المشكلات التقنية حيث ان بعض الجهات الامنية والمخابراتية في سوريا وايران قاموا بتلقيم البرنامج بملفات تجسس يصعب الكشف عنها

لذلك نرجو من الاخوة في سوريا والاحواز المحتل عليهم فقط بتحميل البرنامج من موقعه الرسمي

الان بعون الله نبدأ في شرح برنامج تور و اول خطوة هي التوجه الى الموقع الرسمي للبرنامج من اجل تحميل البرنامج كما تشاهد في الشرح المصور

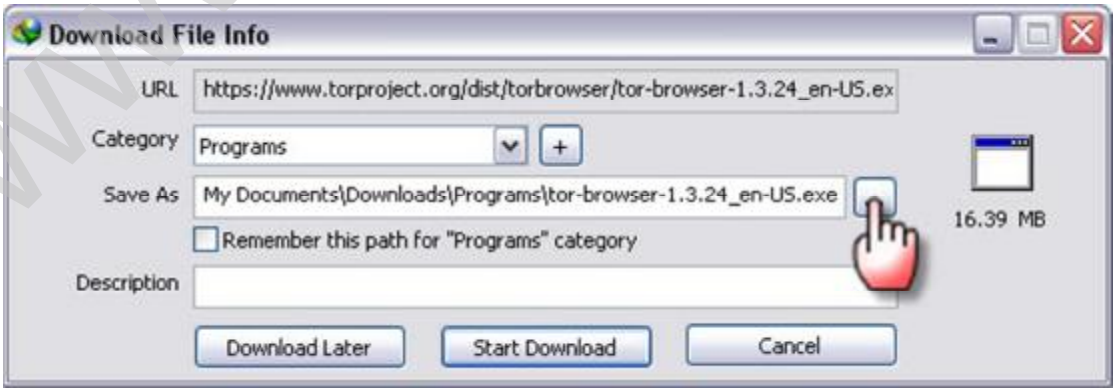
https://www.torproject.org	برنامج
في حالة عدم عمل الرابط في الموضوع تم ارفاق ملف تكست يحتوى على رابط الموقع الرسمي لتحميل البرنامج – اسم الملف TOR-001	

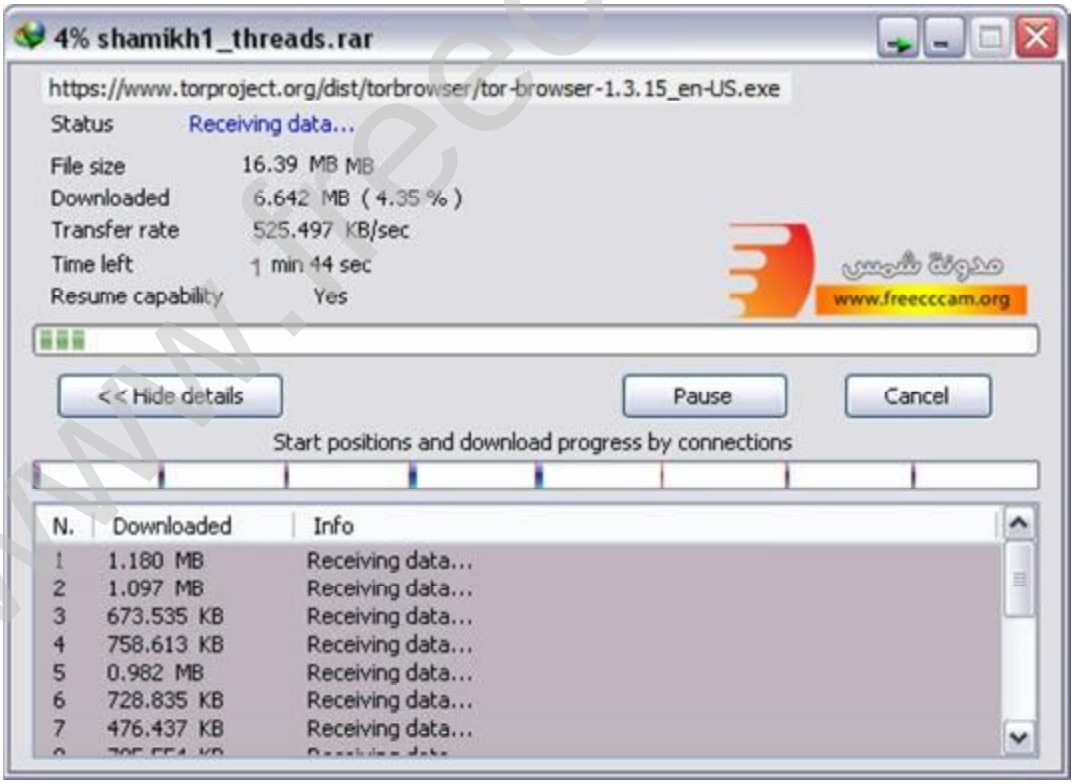


1	البرنامج لنظام التشغيل ويندوز نسخة محمولة
2	البرنامج لنظام التشغيل ويندوز نسخة للتثبيت على الجهاز
3	البرنامج لنظام التشغيل ماك نسخة محمولة
4	البرنامج لنظام التشغيل ماك نسخة للتثبيت على الجهاز
5	i686 البرنامج لنظام التشغيل لينكس
6	x86_64 البرنامج لنظام التشغيل لينكس

الان نقوم بتحميل برنامج ثور تابع الشرح المصور لطريقة تحميل البرنامج

الان يمكنك حفظ البرنامج على الجهاز او حفظ البرنامج في فلاشه خارجية من اجل استعمال البرنامج على أي جهاز اخر وفى أي مكان وفى هذا الشرح سوف نقوم بحفظ البرنامج على الفلاش ميموري

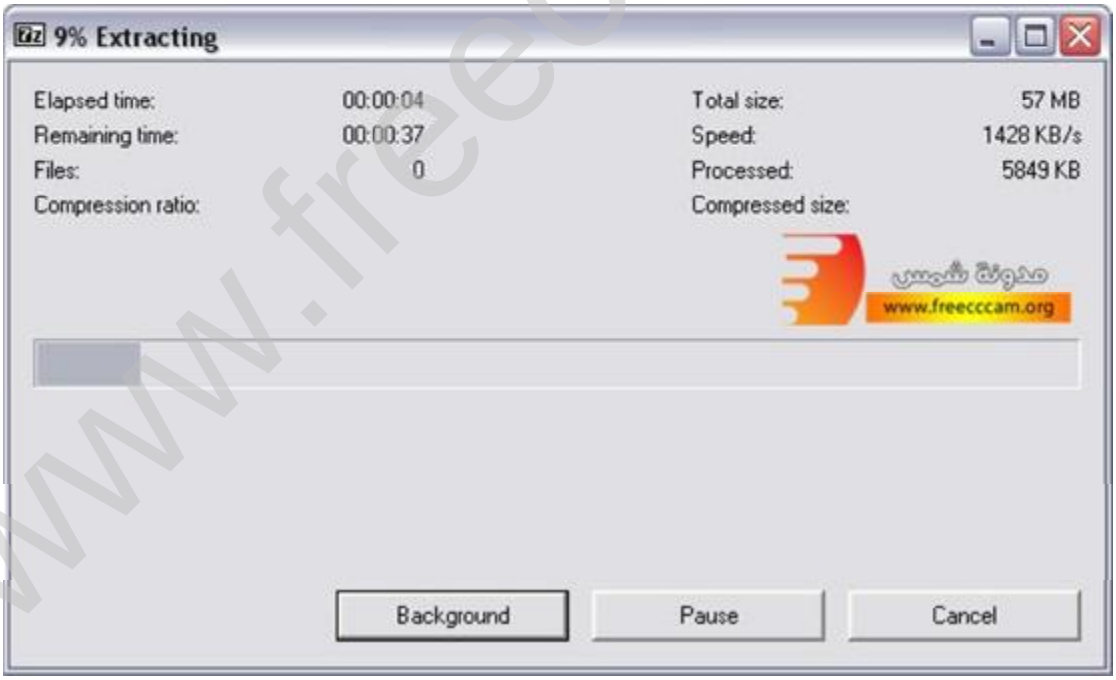




بعد الانتهاء من تحميل البرنامج وحفظة في الفلاش ميموري الان نقوم بفتح الفلاش ميموري ونجد برنامج تور مضغوط

تابع شرح طريقة فك الضغط عن البرنامج فى الفلاش ميمورى

- في الصورة التالية نختار فك الضغط عن البرنامج في الفلاش ميموري



هذا هو البرنامج بعد فك الضغط عنه

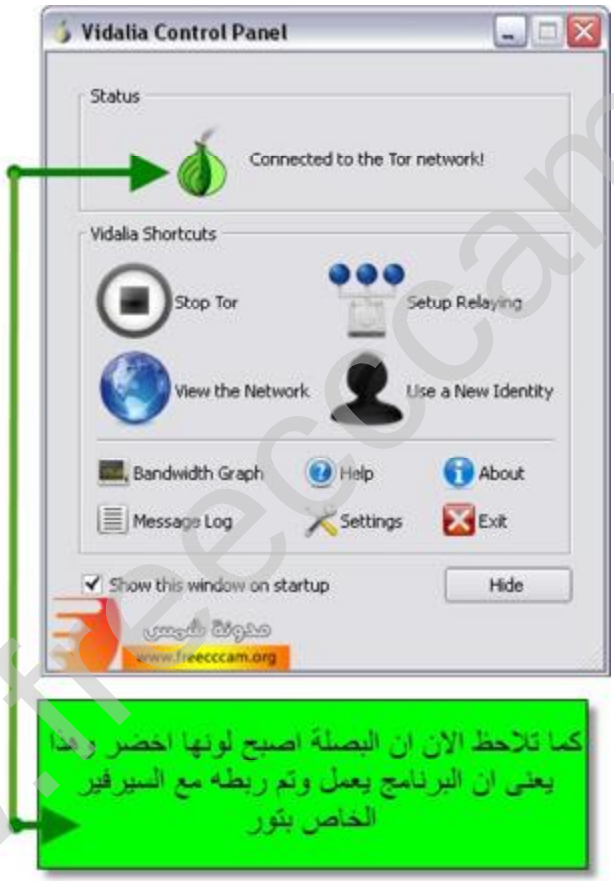
- كما تشاهد الان جميع ملفات برنامج تور بعد فك الضغط عن البرنامج لنتعرف على ملفات برنامج تور قبل البداء بتشغيل البرنامج

Data	هذا المجلد يحوى بعض الملفات التي سوف نحتاج للتعامل والتعديل عليها مستقبلا
FirefoxPortable	هذا مجلد متصفح الفايرفوكس وللعلم ان برنامج تور يأتي معه مدمج المتصفح الرائع الفايرفوكس
Start Tor Browser	هذه الايقونة الرئيسية للبرنامج ومنها نقوم بتشغيل برنامج تور

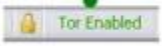
الان نقوم بتشغيل برنامج تور بالضغط دبل كليك على هذه الايقونة

- بعد الضغط على ايقونة تشغيل البرنامج تظهر لنا لوحة تشغيل واعدادات البرنامج كما تشاهد فى الصور التالية

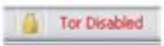
في هذا الشريط المتحرك تشاهد عملية التقدم في ربط وتشغيل برنامج تور



بعد عمل برنامج تور وربطه بشبكة تور سوف يقوم البرنامج بفتح متصفح الفايرفوكس المدمج مع برنامج تور وتشاهد رسالة في المتصفح تهنئة وتعلمك ان البرنامج يعمل بشكل سليم الان كما تشاهد في الصورة التالية



في حالة مشاهدة هذه الكتابة باللون الاخضر هذا يعنى ان البرنامج يعمل وانه يمكنك التصفح بأمان



في حالة مشاهدة هذه الكتابة باللون الاحمر هذا يعنى ان البرنامج لايعمل وانه لايمكنك التصفح بأمان

بعد عمل البرنامج سوف نقوم الان بتغير لغة البرنامج من اللغة الانجليزية الى اللغة العربية