



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

دورة أمن الهواتف الذكية

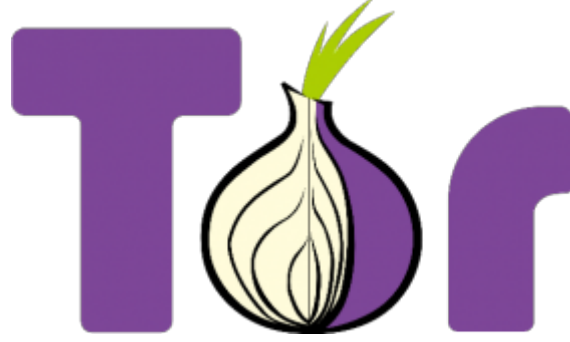
الدرس الثالث

الدليل الشامل لتور أندرويد

الحمد لله معز الاسلام بنصره ومذل الشرك بقهره ومصرف الامور بأمره
ومستدرج الكافرين بمكره الذي قدر الايام دولا بعدله وجعل العافية للمتقين
بفضله والصلاة والسلام علي من أعلي الله منار الاسلام بسيفه وعلي اله

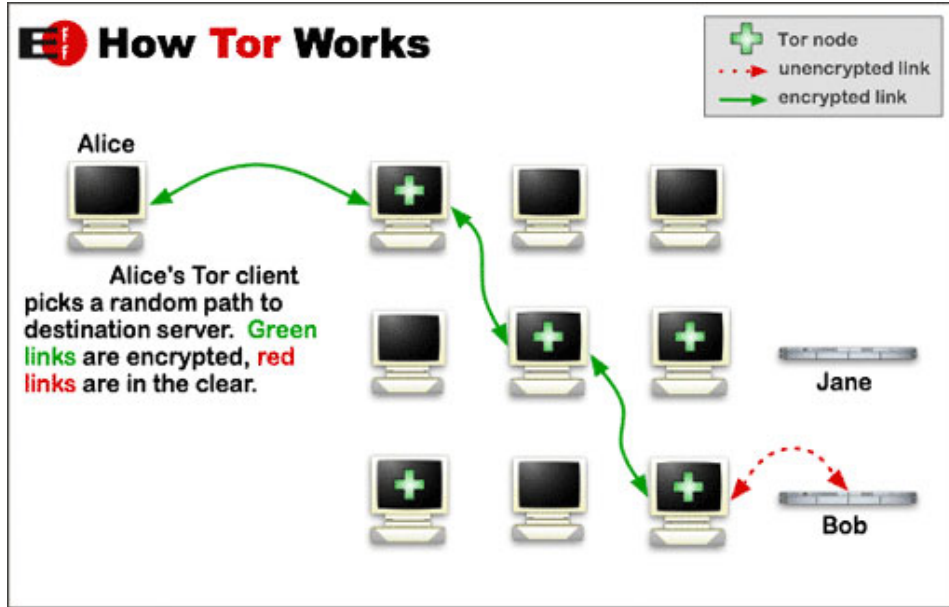
وصحبه ومن تبعهم باحسان الي يوم الدين اما بعد

نبذة عن Tor وألية عمله



ما هو "تور" Tor

تم تطوير برنامج Tor ليؤمن مجهولية الاتصال والخصوصية والأمان لنشاط المستخدمين على الإنترنت حيث يقوم البرنامج بربط المستخدمين مع شبكة Tor والتي تتكون من مجموعة من "العقد" المتداخلة تتم عملية الاتصال عبر هذه العقد للحصول علي الخصوصية التامة وتأمين المستخدمين من تسجيل تحركاتهم علي شبكة الانترنت والمواقع التي يزورونها كما تحميهم من محاولات التعقب وتحديد الهوية وعمليات التجسس التي يمكن ان يقوم بها أفراد او شركات او حكومات



ماذا يعني "عقد" و"شبكة Tor" ؟

شبكة Tor هي مجموعة كبيرة من الأجهزة الشخصية والمخدّمات التي يشغلها متطوعون حول العالم تسمى هذه الأجهزة بالـ "عقد".

يتم اختيار هذه العقد من قبل Tor بشكل عشوائي لتميرير الاتصال وفي كل عملية اتصال يوجد 3 عقد: عقدة دخول، عقدة وسطى، وعقدة خروج ، تمنع هذه الطريقة التي يعمل بها Tor أي شخص يراقب اتصالاتكم بالانترنت من معرفة المواقع والخدمات التي تزورونها ، كما تمنع أيضا هذه المواقع من معرفة موقعكم الجغرافي الحقيقي

عقدة الدخول : في **Tor** تعرف موقعكم الجغرافي، فيما لا تعرف البيانات التي يتم إرسالها لأنها تكون مشفرة قبل دخولها

العقدة الوسطى : لا تعرف أي معلومات (لا مكانكم الجغرافي، ولا البيانات التي أرسلتموها، ولا الموقع الذي تتوجهون إليه) هذه العقدة تعرف فقط أن عليها استقبال البيانات من عقدة الدخول، وتمريرها إلى عقدة الخروج.

عقدة الخروج : تقوم بفك تشفير البيانات وتمريرها إلى الموقع، لذا عقدة الخروج تعرف الموقع الذي تودون زيارته، والبيانات التي ترسلوها لتمريرها إلى الموقع. ولكن في حال استخدامكم **Tor** في موقع يدعم تشفير HTTPS فإن عقدة الخروج تستطيع معرفة الموقع الذي تريدون زيارته فقط، فيما يتم فك تشفير البيانات على مخدّم الموقع الذي قمتم بزيارته

 **Tor** الخاص بنظام التشغيل أندرويد من متجر

اضغط هنا وللتحميل المباشر **اضغط هنا**

تنبيه هام : التطبيق يحتاج الي روت ليعمل بشكل صحيح اذا لم تعرف ما الروت او كيفية تثبيته **اضغط هنا**



مؤخراً **Tor** لم يكن يعمل علي اجهزة اندرويد الا بصلاحيه الروت اما الان فأضيفت خدمة الVPN والتي تشفر اتصالك بالانترنت عن طريق شبكة



لتفعيل هذه الخدمة اضغط علي كلمة APPS في الصورة السابقة ثم اضغط
ACTIVATE وستلاحظ ظهور ايقونة مفتاح في مكان الاشعارات وهذا
يدل علي ان التطبيق يعمل

تنبيه هام : خدمة APPS مازالت تجريبية لذا لن تعمل بشكل مناسب علي
جميع الاجهزة وربما تتوقف تلقائيا ولا يُنصح باستخدامها في التخفي لانها
صممت لتجاوز الجدران النارية والفلاتر

Download
0kbps / 0KB

Upload
0kbps / 0KB



Apps Mode

You can enable all apps on your device to run through the Tor network using the VPN feature of Android.

WARNING This is a new, experimental feature and in some cases may not start automatically, or may stop. It should NOT be used for anonymity, and ONLY used for getting through firewalls and filters.

CANCEL ACTIVATE

- long press to start -

CHECK BROWSER

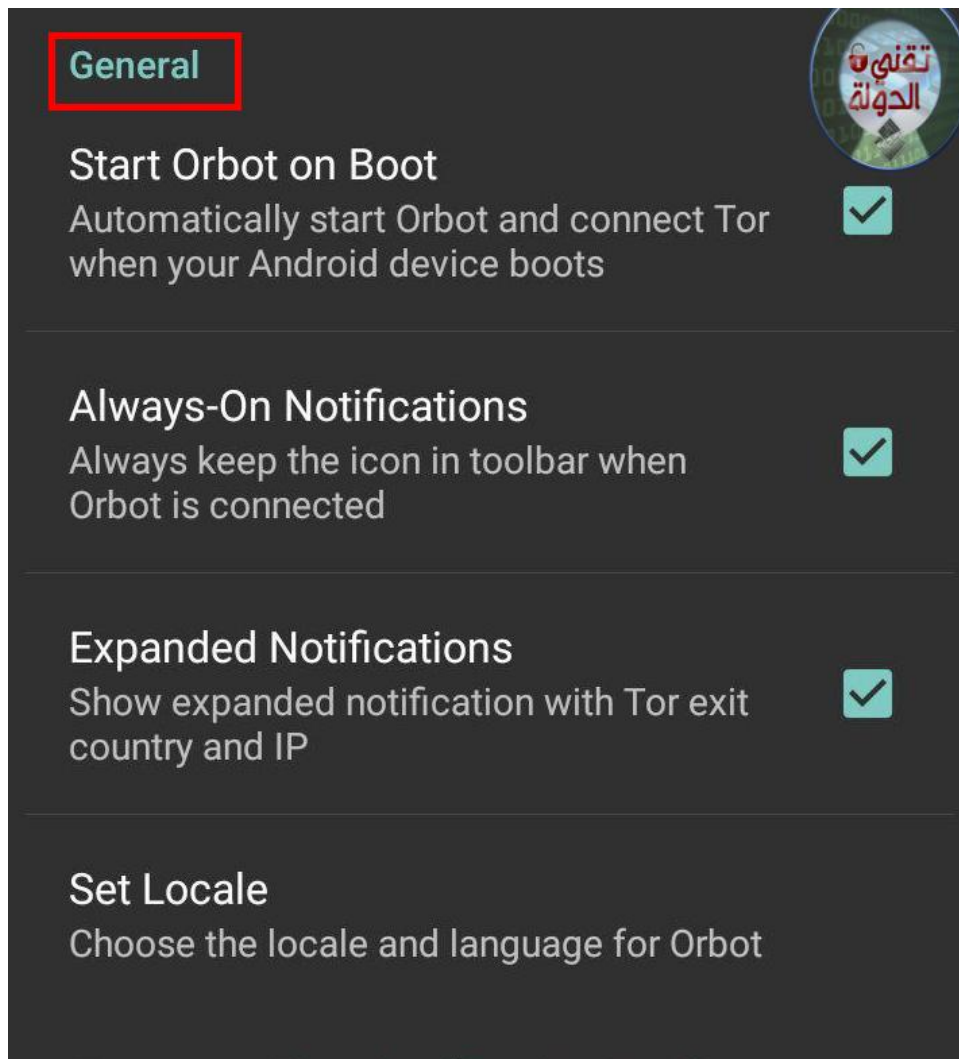
APPS

BRIDGES

إضغط هنا للذهاب إلي إعدادات التطبيق



المرحلة الأولى : الاعدادات العامة General



1- Start Orbot On Boot

لتشغيل التطبيق تلقائياً عند إعادة تشغيل الهاتف

2- Always -on notifications

تثبيت ايقونة التطبيق في منطقة الاشعارات

3- Expand notifications

تظهر لك رسالة في منطقة الاشعارات بها عنوان IP الحالي والبلد
ال

4- set locale

لتغيير لغة التطبيق ولكن بعد اختيار لغة جديدة اخرج من التطبيق
وافتحه مجددا لتغيير اللغة

المرحلة الثانية : بروكسي ضمني **Transparent Proxying**

Transparent Proxying (Requires Root)

Request Root Access

Request root access for transparent proxying



Transparent Proxying

Automatic Torifying of Apps



Tor Everything

Proxy traffic for all apps through Tor



Select Apps

Choose Apps to Route Through Tor

Tor Tethering

Enable Tor Transparent Proxying for Wifi and USB Tethered Devices (requires restart)



1- Request Root Access

يطلب إذن روت

2- Transparent Proxing

بروكسي ضمني

3- Tor Everything

بروكسي تور في جميع التطبيقات – لا تحتاج لاضافة بروكسي يدوي للتطبيقات في هذا الخيار

4- Select Apps

اختيار تطبيقات معينة لتشفير اتصالاتها

5- Tor Tethering

بروكسي ضمني للاتصال بالانترنت عن طريق الواي فاي او USB ال

تنبيه هام: بتفعيل بروكسي ضمني يتم تشفير اتصال جميع التطبيقات ولا تحتاج لاضافة بروكسي يدويا الي التطبيقات كتويتر وفايرفوكس

المرحلة الثالثة : إعداد العُقد Node Configuration

Node Configuration



Entrance Nodes

Fingerprints, nicks, countries and addresses for the first hop

Exit Nodes

Fingerprints, nicks, countries and addresses for the last hop

Exclude Nodes

Fingerprints, nicks, countries and addresses to exclude

Strict Nodes

Use *only* these specified nodes



ملاحظة: شرحنا سابقا معني العقد وانواعها ويمكننا تحديد في اي بلد تريد بياناتك واتصالاتك ان تمر بها من خلال اضافة اختصارات الدول لكل عقدة

1- Entrance Nodes

يقوم هذا الخيار بإخبار **Tor** أن عليه المرور فقط من عقد الدخول والمنتصف الموجودة في الدول المحددة

هذا السطر الذي بالاسفل به اختصار لعدة دول اوروبية واسترالية هي الافضل في حماية الخصوصية مثل سويسرا ورومانيا واستراليا

قم بنسخ ولصق السطر في خانة ال **Entrance Nodes**

```
{ch} , {fi} , {ro} , {no} ,  
{au} , {nl}
```

2- Exit Nodes

عقدة الخروج يقوم هذا الخيار بإخبار "تور" أن عليه المرور فقط من عقد الخروج الموجودة في الدول المحددة

اضف القائمة السابقة من اختصارات الدول في **Exit Nodes** خانة ال

3- Exclude Nodes

يقوم هذا الخيار بإخبار

أن عليه تفادي المرور من عقد الخروج الموجودة في الدول **Tor** المحددة

اضف هذه الدول بهذا الخيار

{us} , {uk} , {ru} , {sy} , {eg} , {sa} , {tn}

هذه اختصارات امريكا والولايات المتحدة وروسيا وسوريا ومصر والسعودية وتونس لذا قم باضافة اختصار بلدك مع هذه البلاد لتمنع مرور اتصالك منها وهذا رابط به اختصارات جميع الدول [اضغط هنا](#)

4- Strict Nodes

هذا الخيار يتعلق بخيار "ExcludeNodes" ويحتمل هذا الخيار التعطيل او التفعيل في حال تفعيله فاتصالك لن يمر بالدول التي وضعتها في خانة الEXclude Nodes

المرحلة الرابعة: إضافة الجسور Bridges

Bridges

Use Bridges

Enable alternate entrance nodes into the Tor Network



Bridges

IP address and port of bridges

1- Use Bridges

تفعيل الجسور والجسور هي مجموعة من العقد تتصل بشبكة تور وتعمل كعقد دخول ولا يمكن حجبها من قبل مزود الخدمة أو الحكومة

2- Bridges

إضافة الجسور من خلال الذهاب الي هذا الرابط

ثم تابع الخطوات التالية



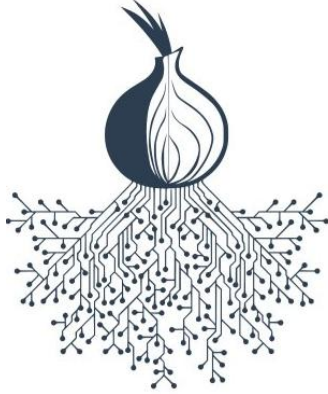
Step 1 Download [Tor Browser](#)

Step 2 Get [bridges](#)

Step 3 Now [add the bridges to Tor Browser](#)

What are bridges?

[Bridges](#) are Tor relays that help you circumvent censorship.



Get Bridges!



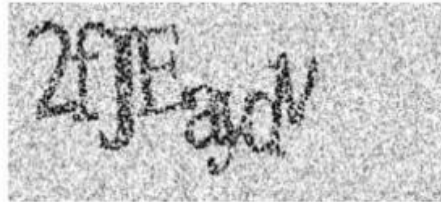
BridgeDB can provide bridges with several [types of Pluggable Transports](#), which can help obfuscate your connections to the Tor Network, making it more difficult for anyone watching your internet traffic to determine that you are using Tor.

Some bridges with IPv6 addresses are also available, though some Pluggable Transports aren't IPv6 compatible.

Additionally, BridgeDB has plenty of plain-of-vanilla bridges – without any Pluggable Transports – which maybe doesn't sound as cool, but they can still help to circumvent internet censorship in many cases.

Just give me bridges!

في الصورة التالية اكتب الرمز الذي في الصورة ثم اضغط علي السهم



Enter the characters from the image above...



في تطبيق اوربوت

Bridges

في الصورة التالية الارقام التي باللون الاحمر هي الجسور قم بنسخ
جسر ولصقه في خيار



bridges

Here are your bridge lines:

52.8.110.121:8443	D0D19C131E4006099D0D0F5D8320028489262B82
69.59.152.157:9001	4E1464B5D5701066F4422FFB1780CF7448E2DAAE
148.66.82.221:443	E83FC79027E2161E3971D159A8D435AA2D48289C

Select All Show QRCode

How to test using your bridges

واخر دعوانا ان الحمد لله رب العالمين

لا تنسونا من صالح دعائكم



للدعم الفني تواصل معي علي



SR444TAW



@SOFTWARE_ENG

للمزيد من الدروس والاطخبار الامنية تابعونا علي قناة المكتبة التقنية

المكتبة التقنية
TECHNICAL LIBRARY

قناة تقنية تنشر دروس ودورات في مجال
الحماية الإلكترونية وأمن المعلومات .

 [TELEGRAM.ME/TECH_LIB](https://t.me/TECH_LIB)

