Como Navegar nas Redes Onion e I2P da Deep Web

O objetivo deste tutorial é capacitar os usuários a navegarem nas camadas Onion e I2P do que é conhecido como Deep Web (conjunto de sites que não são identificados pelos buscadores comuns, tais como Google, Bing e Yahoo).

Foram escolhidas as duas camadas acima citadas devido à baixa complexidade de configurações necessárias para que se realize a navegação por elas, de maneira que se trata de um tutorial para usuários que desejam dar seus primeiros passos no tema da navegação criptografada.

Espera-se que esta leitura sirva para a tarefa a que se propõe, de proporcionar aos usuários ferramentas a mais às suas pesquisas na Internet, e assim crescerem no conhecimento avançado de Informática, de hacking e também nas interações relacionadas à ideia Anonymous.

Cuidados com a segurança:

Assim como na navegação na superfície, na Deep Web (independentemente da rede na qual se esteja) são necessários cuidados no que diz respeito à proteção.

Seguem, abaixo, por tanto, algumas sugestões de itens essenciais para que se consiga uma navegação segura e com menor potencial de percalços como invasões ou infecções:

Comodo Firewall (gratuito) : http://personalfirewall.comodo.com/

Norton Internet Security 2013 (pago): http://br.norton.com/internet-security/

Kaspersky Internet Security 2013 (pago): http://www.kaspersky.com/pt/internet-security

Valhala Honeypot (grátis. A versão atual enquanto se escreve este tutorial é a 1.8: http://valhalahoneypot.sourceforge.net/

Sugerimos o investimento financeiro em segurança sempre que possível. Softwares pagos além de oferecerem mecanismos de proteção com atualizações dedicadas e em tempo real, oferecem também suporte técnico especializado e de pronto atendimento.

O Que é a Rede Onion?

"The Onion Router, também conhecido pela sigla TOR, é uma rede de computadores distribuída com o intuito de prover meios de comunicação anônima na Internet. A maioria das distribuições GNU/Linux disponibilizam pacotes do Tor, embora haja versões para diferentes sistemas operacionais, tais como Windows e Mac OS. A rede TOR é uma rede de túneis http (com tls) sobrejacente à Internet, onde os roteadores da rede são computadores de usuários comuns rodando um programa e com acesso web (apenas). O objetivo principal do projeto é garantir o anonimato do usuário que está acessando a web". (Fonte: http://pt.wikipedia.org/wiki/The_Onion_Router).

TOR[1] foi originalmente concebido, implementado e implantado como um projeto de roteamento do Laboratório de Pesquisa Naval dos EUA. A rede TOR foi originalmente desenvolvida com a Marinha dos EUA em mente, tendo como objetivo principal proteger as comunicações do governo. Hoje, esta rede é utilizada todos os dias por uma grande variedade de propósitos por pessoas normais, militares, jornalistas, policiais, ativistas e muitos outros.

TOR, portanto, é uma rede de túneis virtuais que permite a pessoas e organizações aumentar a sua segurança e privacidade na Internet. Esta rede também permite a desenvolvedores de software para criar novas ferramentas de comunicação com características "built-in" de privacidade. TOR fornece a base para uma gama de aplicações que possibilitam que organizações e particulares partilhem informações através de redes públicas sem comprometer a sua privacidade.

Serviços ocultos da rede TOR permitem aos seus utilizadores a publicação de sites web e outros serviços sem a necessidade de revelar a localização original dos mesmos.

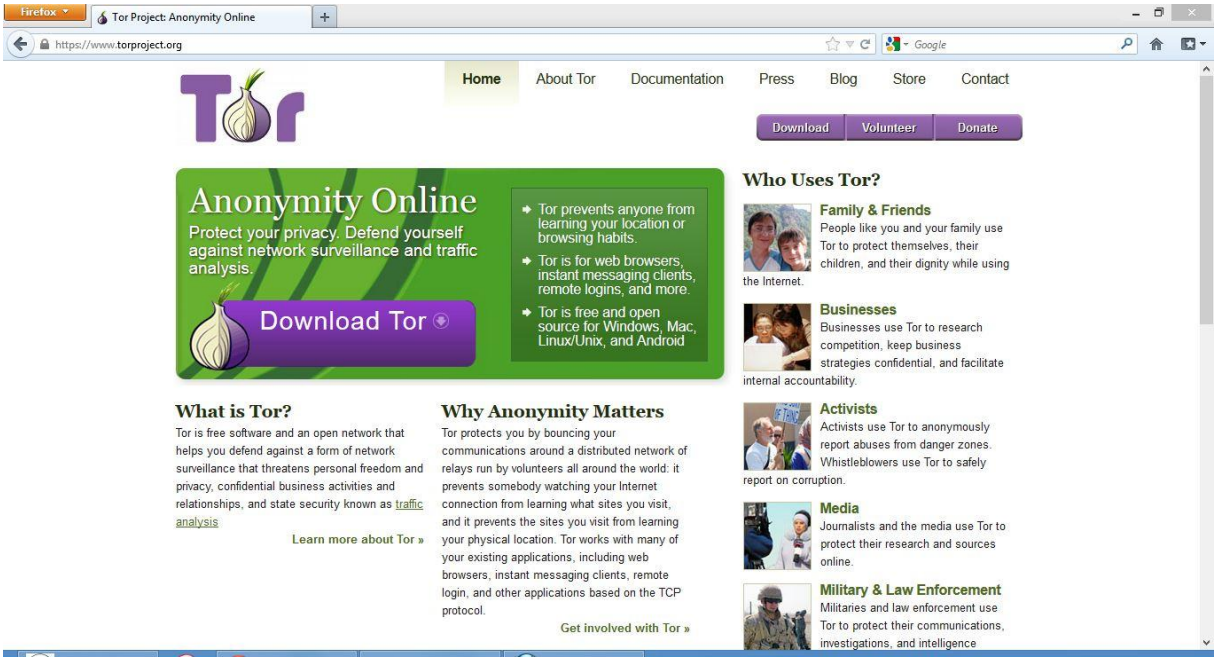
[1] Este parágrafo e seus dois seguintes consistem em uma versão adaptada do texto original disponível no site oficial do Projeto TOR, cujo endereço é: https://www.torproject.org/about/overview.html.en

Com base nas descrições acima, fica mais fácil concluir que ao utilizar-se o tão famoso navegador TOR, estamos realizando uma navegação por meio de um browser capaz de interagir com a rede Onion. Isso explica, também, a razão de a terminação dos links que fazem partes dessa rede terminem com a extensão *.onion*, e também o fato de tais links não serem compostos por palavras como acontece em sites da WEB comum, e sim por meio de letras e números misturados entre si, que é uma característica da criptografia utilizada pela rede em questão.

Como Rodar o Navegador TOR no Windows

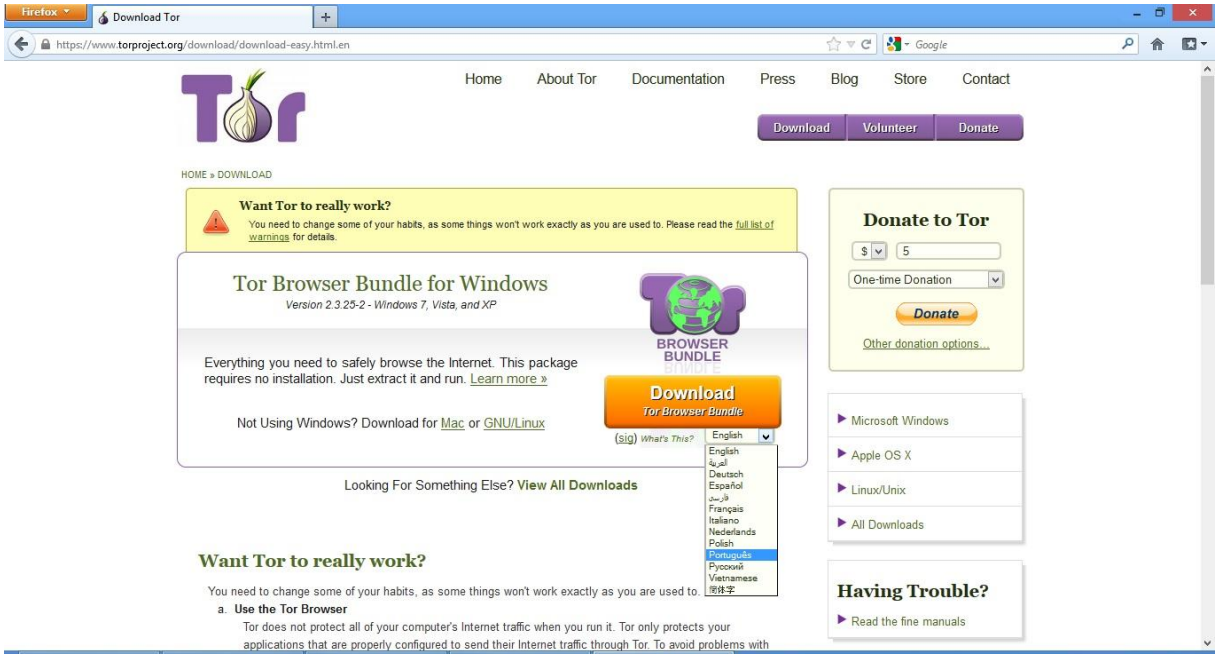
É importante ressaltar que o foco deste tutorial reside na plataforma Windows, mas o leitor que quiser rodar o navegador TOR em sistemas Linux, temos também já publicado um tutorial bastante ilustrado para isso, cujo link para download é este[2]:
https://www.facebook.com/groups/GdELackingFaces/538200659525949/

O primeiro passo para se adquirir o navegador TOR consiste em realizarmos seu download (gratuito, obviamente), no site oficial de seu projeto, cujo endereço é: https://www.torproject.org/. Logo na página inicial já é oferecido download do pacote completo de arquivos necessários para rodar o navegador, como pode ser visto na figura abaixo:



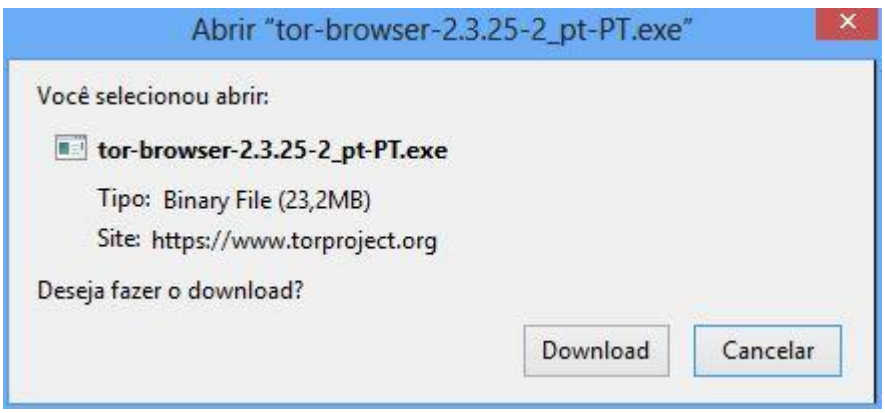
[2] Embora o tutorial apontado no link seja destinado à distribuição Backtrack 5, os passos nele contidos podem ser aproveitados para qualquer outra distribuição Linux.

Tendo, portanto, acessado o site apontado acima, basta clicarmos no botão na cor Roxo, no qual consta a descrição “Download Tor”, para que sejamos encaminhados para a página seguinte:

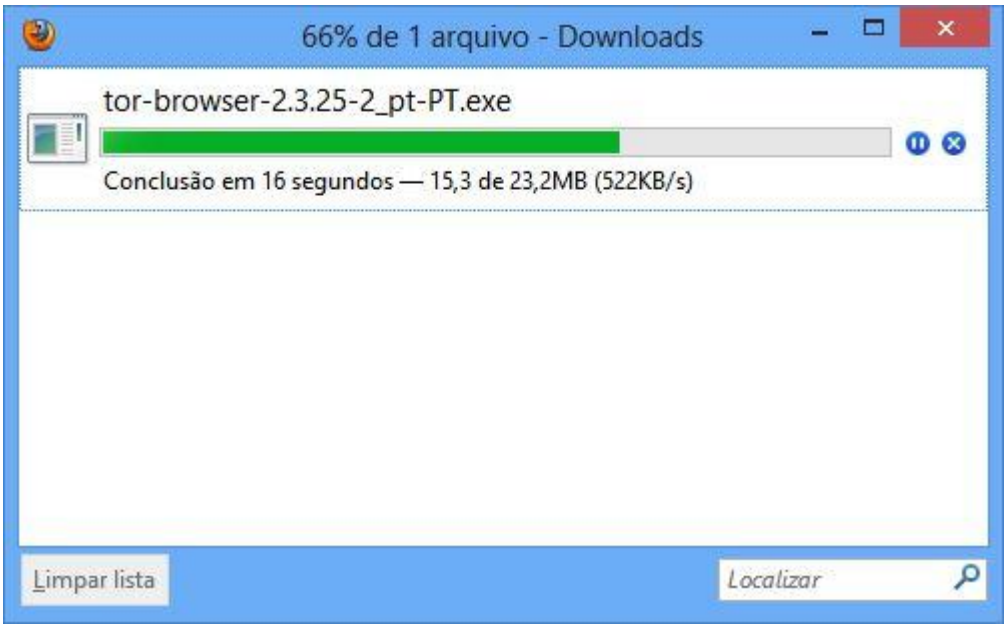


Podemos escolher o idioma do TOR, como pode ser visto na imagem acima, ao clicar na pequena lista que aparece abaixo do botão laranja de Download. Após selecionado o idioma, clica-se no botão para começar a baixar. É interessante observar que embora não conste na descrição do site, o TOR já é compatível com o Windows 8.

Abaixo segue a janela de início do download (o navegador utilizado neste tutorial, como pode se presumir, é o Mozilla Firefox 18.0:



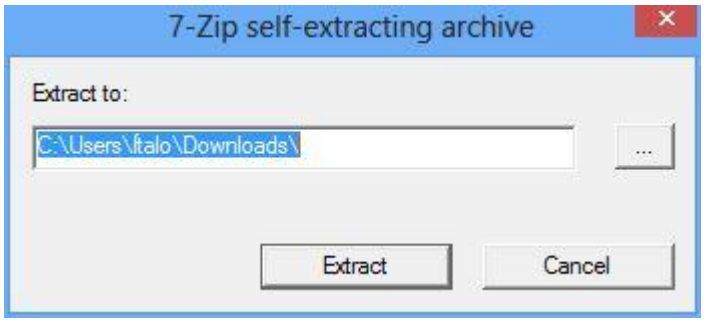
Aqui, portanto, segue a imagem do download em andamento:



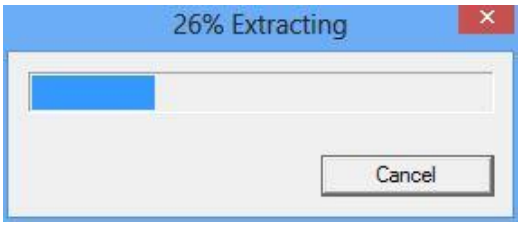
Após terminado o download, basta procurarmos o pacote de arquivos baixado, que se encontrará na pasta na qual comumente os downloads realizados pelo navegador são armazenados. No caso deste tutorial, o arquivo baixado foi para a pasta “Downloads” do Windows 8 PRO, como se pode ver na figura abaixo:

Como se pode ver na figura acima, o arquivo baixado contendo o conjunto completo de arquivos necessários para a execução correta para usuários finais do TOR se encontra compactado. Devemos, portanto, descompactar o arquivo para podermos acessar seu

conteúdo. Não consiste num procedimento complexo; basta clicarmos duas vezes no pacote, que será apresentada uma janela nos questionando sobre onde queremos que os arquivos descompactados fiquem, como se vê a seguir:

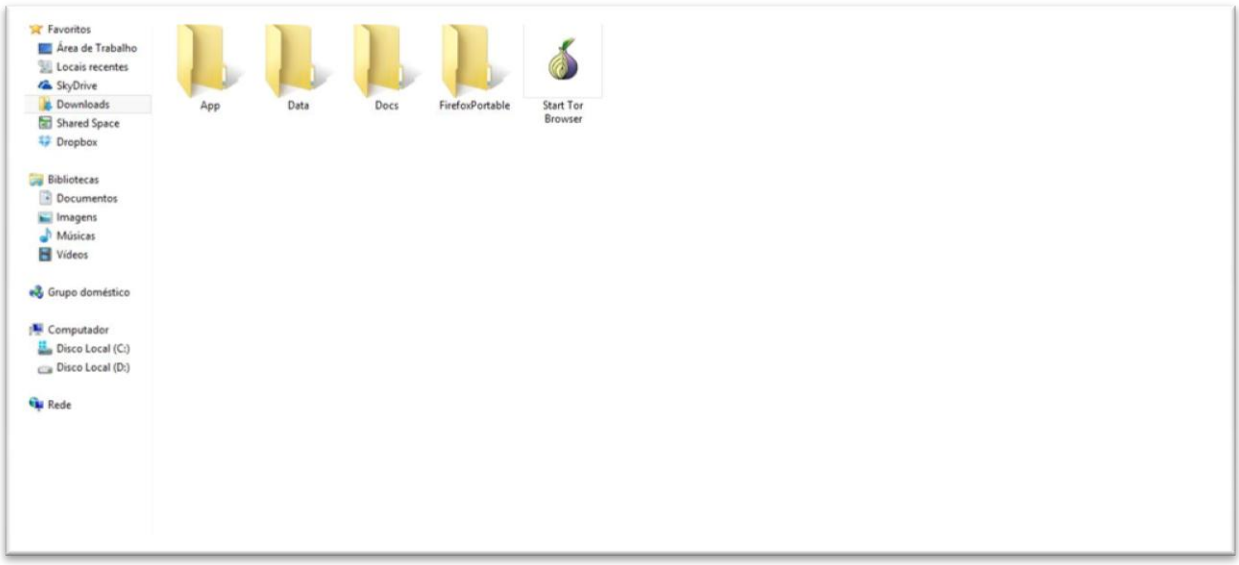


Para este tutorial, optamos por enviar os arquivos na mesma pasta, ou seja, a “Downloads”. Ao clicarmos em Extract, então, a descompactação se iniciará, assim:



Terminada a extração, o usuário verá que na pasta apontada anteriormente constará uma nova pasta, como se vê abaixo:

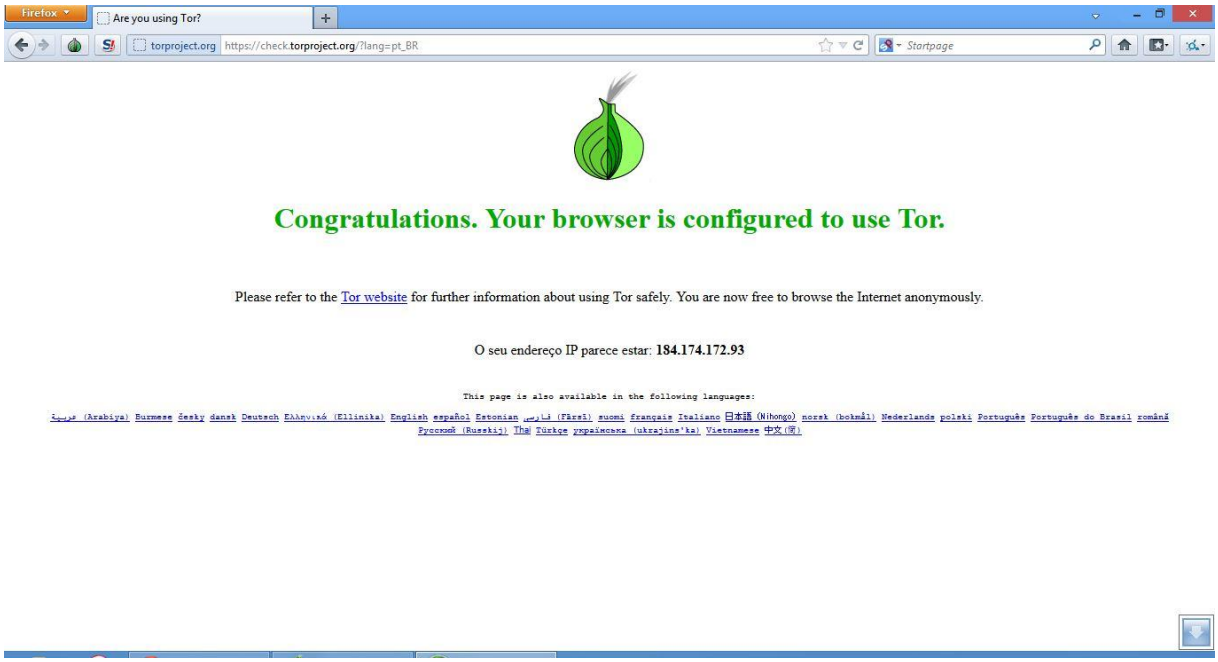
Como se pode ver na imagem acima, o nome da pasta criada automaticamente chama-se Tor Browser. Entramos nesta pasta, e então, lá deverão constar os arquivos conforme se vê na figura a seguir:



O procedimento a partir de agora é bastante simples. Consiste em executarmos o programa cujo nome é Start Tor Browser, que tem como ícone uma cebola.

Com isso, será iniciado o Painel de Controle do Vidalia, assim:

Após a barra de progresso haver chegado no final, é só aguardar alguns segundos para que uma versão adaptada do Mozilla Firefox seja aberta automaticamente, exibindo a seguinte mensagem:

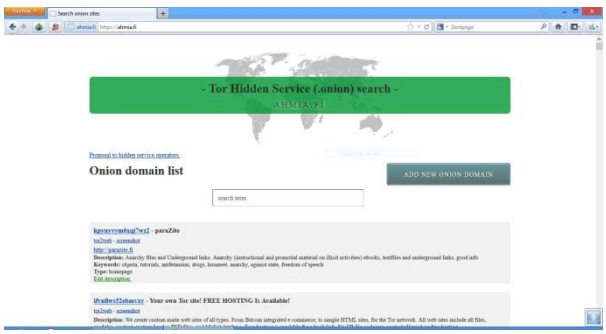


Esta mensagem diz que o navegador em questão está configurado para usar o TOR.

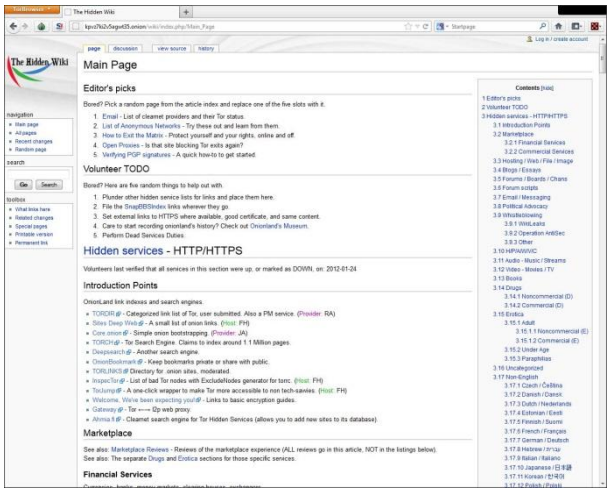
A partir deste ponto o usuário já está pronto para navegar em páginas da rede Onion! Missão cumprida!

Para finalizarmos esta etapa do tutorial, deixamos abaixo algumas sugestões de sites onion para os usuários iniciarem suas pesquisas de maneira qualitativa, buscando manter o melhor foco possível no conteúdo desejado:

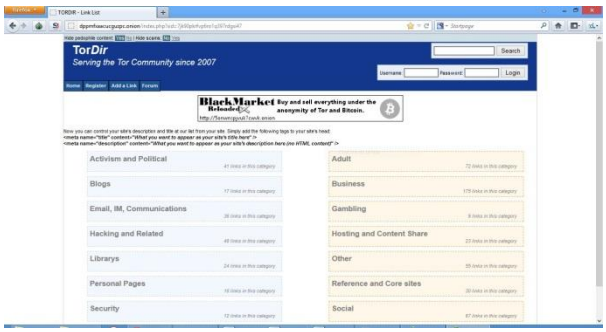
Ahamia.fi: (https://ahmia.fi) – Um motor de buscas similar ao Google, porém destinado a exibir somente sites onion em seus resultados de busca.



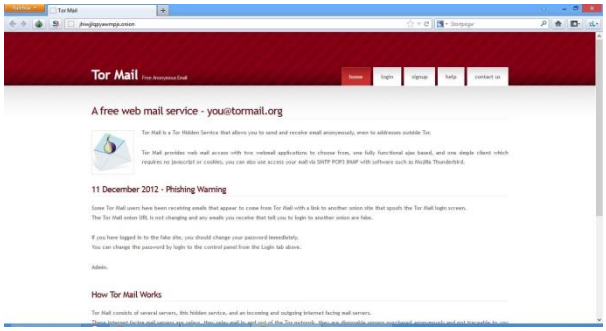
Hidden Wiki: (http://hmybz2age7whj7qr.onion) - coleção de links para outros sites e artigos de enciclopédia em um formato wiki.



TOR Dir: **(http://dppmfxaacucguzpc.onion/) –** Site que indexa outros sites da onion, organizando-os por área temática.



TOR Mail – (http://jhiwjjlqpyawmpjx.onion/) – Serviço de webmail anônimo, muito bom. Grátis, fácil de cadastrar e de manusear.



Por fim, pensamos que com estas orientações o usuário já pode navegar na rede Onion para buscar maiores conhecimentos e acessar meios de comunicação que supram suas necessidades de anonimato.

A próxima etapa deste tutorial, portanto, irá tratar sobre a rede I2P.

O que é a rede I2P?

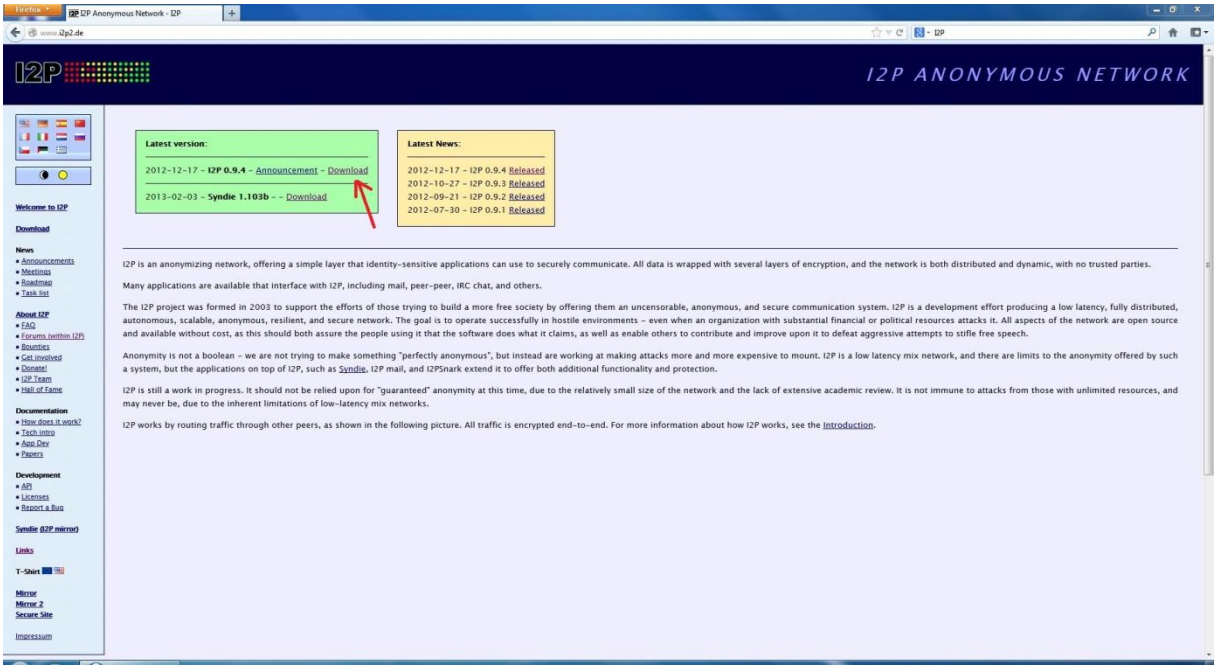
I2P (Invisible Internet Project, que em na notação de pseudo-matemática é representado como I²P.) é uma camada de rede de computador que permite a aplicativos enviar mensagens de maneira segura e com uso de pseudônimos. Nesta camada de rede, portanto, incluem-se atividades tais como navegação anônima na web, utilização de blogs e transferências de arquivos. O software que implementa essa camada é chamado de roteador I2P e um computador com I2P é chamado de nó I2P (ou nodo I2P). O software é gratuito e de código aberto e foi publicado sob várias licenças[3].

Como Rodar o I2P no Windows

Primeiramente, é necessário realizar download do roteador I2P no seu site oficial, cujo link para download é: http://www.i2p2.de/

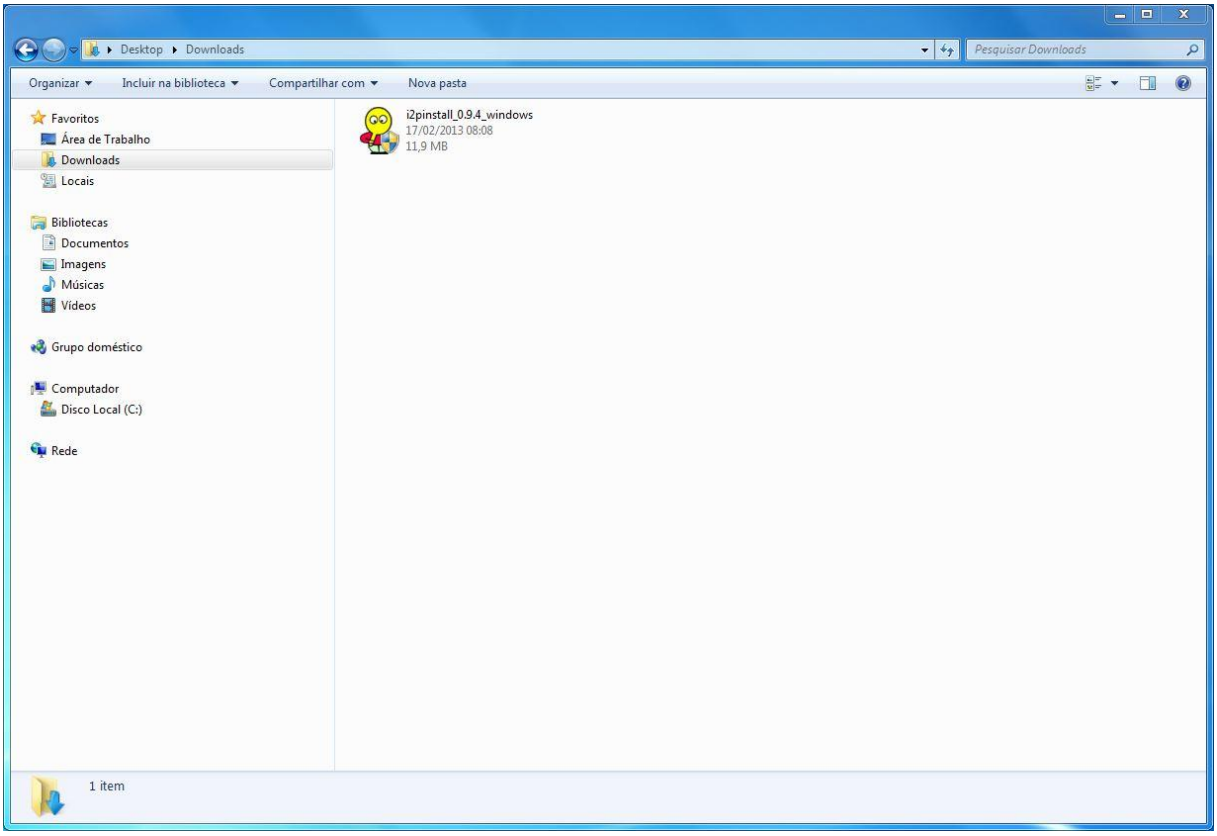
Na página inicial do site já está disponível o link para download, o qual está sendo apontado na figura abaixo:

[3] Maiores informações em: http://en.wikipedia.org/wiki/I2P



Ao clicar no link acima apontado, o usuário será levado para uma nova página, na qual deverá escolher o tipo de arquivo a ser baixado. Como este tutorial é para Windows, então a opção correta é a que se mostra nesta figura:

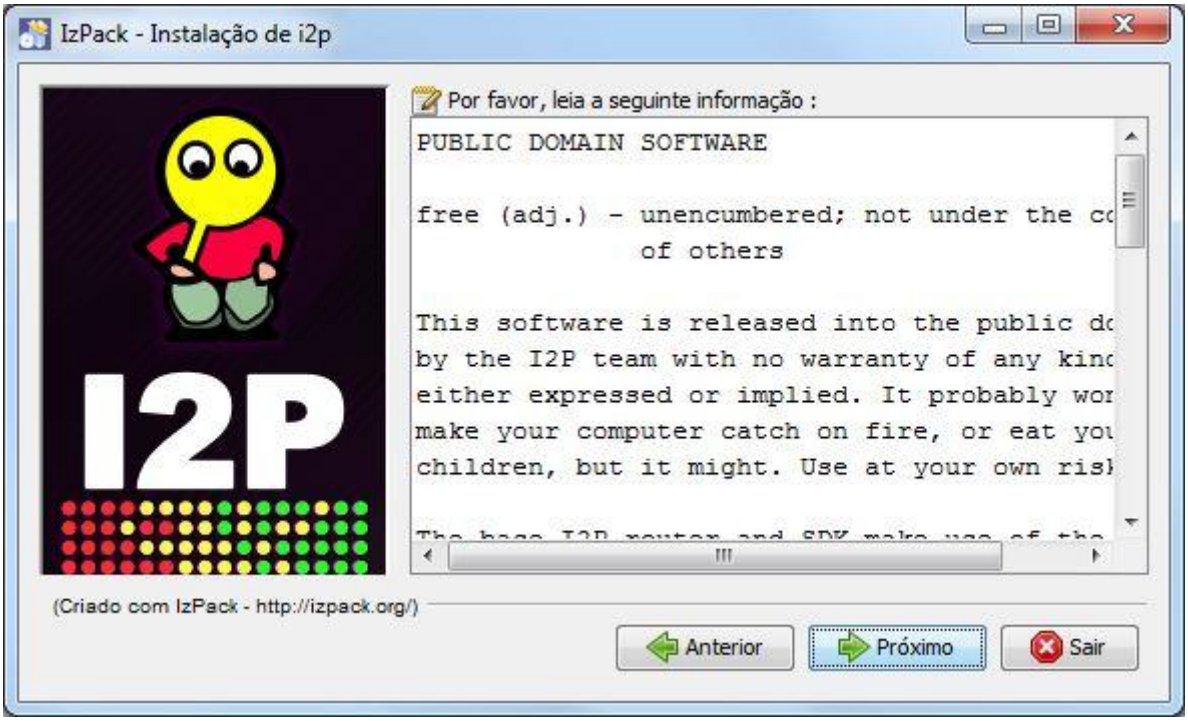
Após realizado o download, o usuário terá o seguinte arquivo:



Clica-se duas vezes em cima do arquivo exibido na figura acima (o qual consiste no instalador do roteador I2P), e então o processo de instalação será iniciado, e a primeira janela do processo será aberta, como se vê na imagem a seguir:

Como se pode ver, trata-se da escolha do idioma da instalação. No nosso caso, escolheremos o idioma Português, e clicaremos em OK, de maneira que será exibida a seguinte janela:

A janela exibida acima nada mais é do que uma mensagem de boas vindas à instalação do I2P. Nela clicamos em "Próximo", e será exibida a próxima janela:



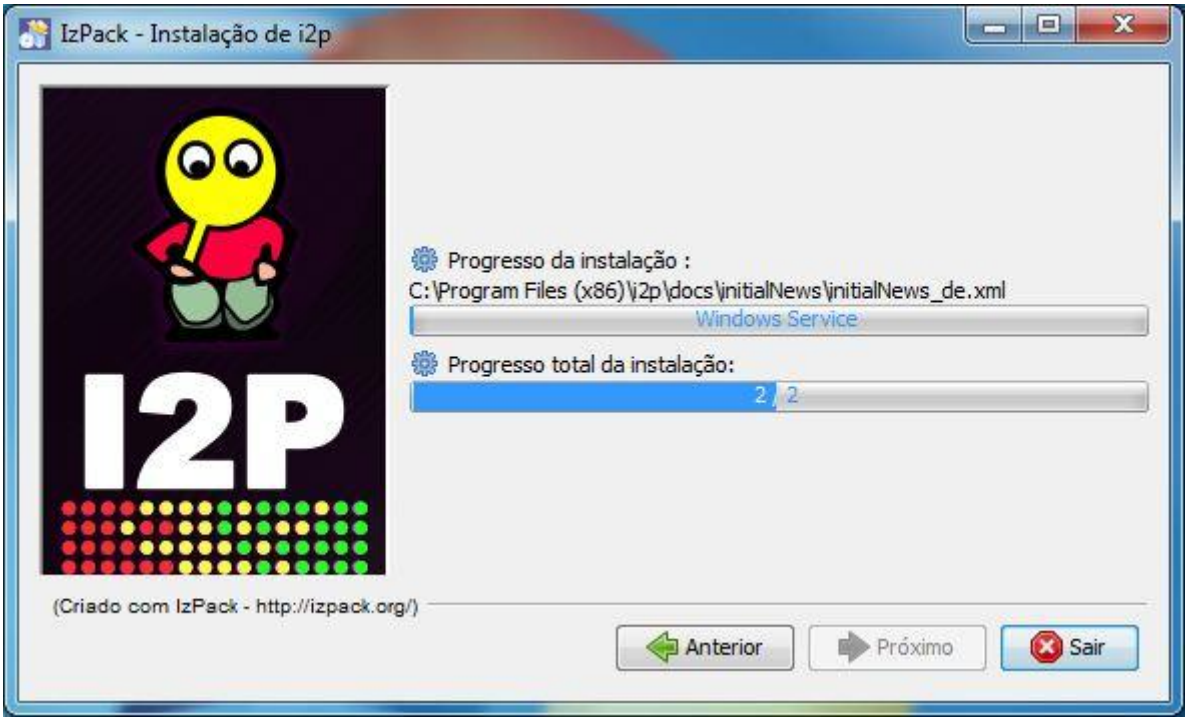
Trata-se do contrato de licença do programa, na qual consta a informação de que se trata de um software de domínio público. Clicamos em "Próximo", e a janela que aparece é a seguinte:

Nessa janela deixaremos marcadas as duas opções, como se vê na figura acima, e clicamos em "Próximo".

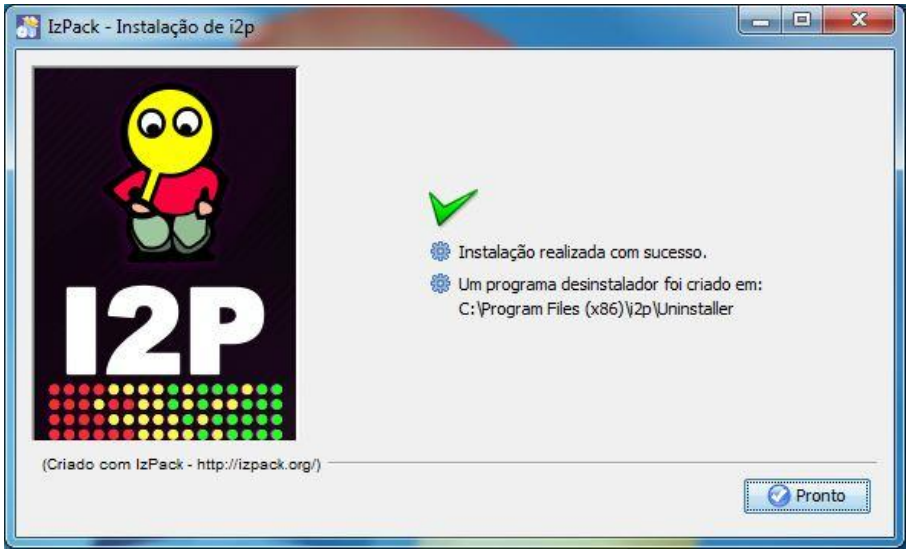
A janela que se apresenta, então, e a seguinte:

Como se vê na figura acima, o campo "Selecione o caminho para instalação" demonstra em qual pasta o programa será instalado. Caso os usuários queiram alterar o destino da instalação, basta clicar em "Procurar" e então escolher outra pasta do computador. Após ter como certa a pasta na qual o programa ficará armazenado, é só clicar em "Próximo", para que se apresente a seguinte janela:

Nesta janela, deixamos marcadas as opções referentes à adição de atalhos na Desktop. Quem desejar alterar o nome do grupo de programas no qual ficarão os atalho do I2P, pode fazê-lo nessa janela, e, depois disso clicar em "Próximo", para que sejam exibidas as barras de progresso da instalação, assim:



A mensagem final de sucesso da instalação pode ser vista abaixo:



Nela, portanto, basta que se clique em "Pronto".

Serão criados os seguintes atalhos na Área de trabalho do Windows:

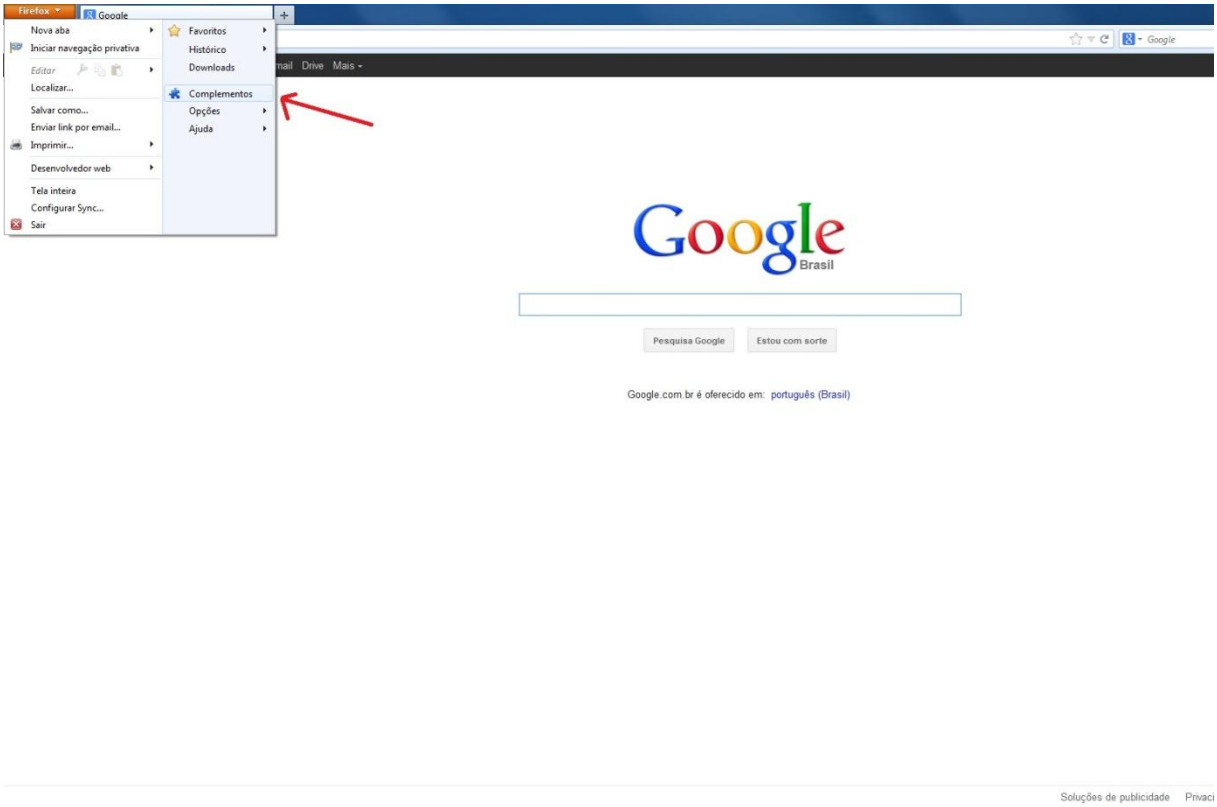
Mas ainda não estamos com tudo pronto para iniciar a navegação na rede I2P. É necessário que adicionemos um complemento em nosso navegador para que possamos navegar utilizando a porta da I2P.

Neste tutorial foi utilizado o Mozilla Firefox como navegador.

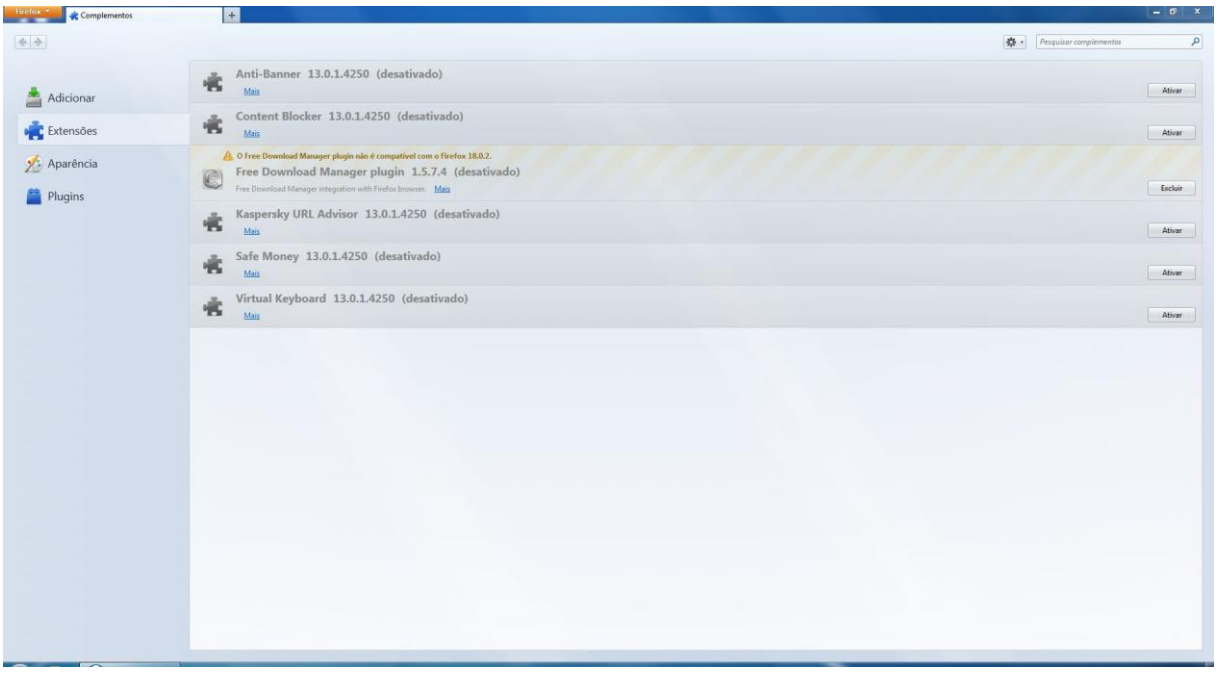
O nome do complemento que utilizaremos se chama Foxy Proxy, e para instalá-lo no Firefox, é necessário realizar os passos que são descritos a seguir:

Como instalar o Foxy Proxy no Mozilla Firefox:

Abre-se uma nova janela do navegador Mozilla Firefox (a versão utilizada neste tutorial foi a 18.0.2), e no canto superior esquerdo da janela dele, clica-se no botão laranja "Firefox". No menu que aparece, clica-se em "Complementos", como mostrado na figura abaixo:

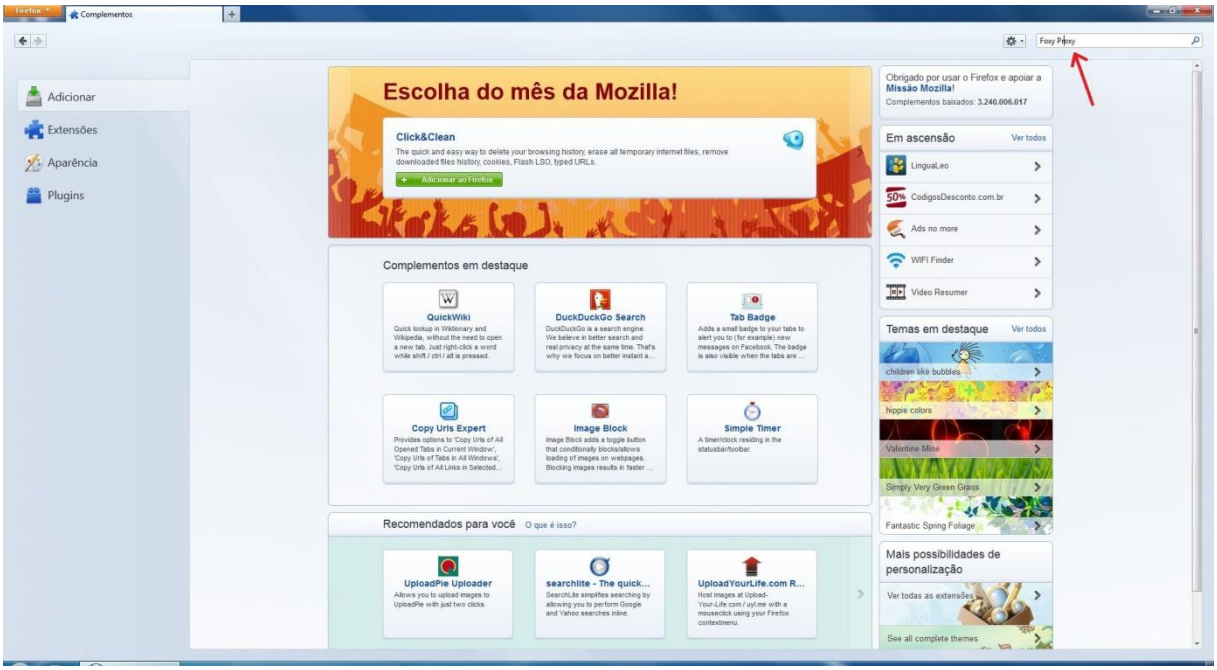


Isso fará com que seja exibida a janela de complementos que já estão instalados no Firefox, mais ou menos assim:

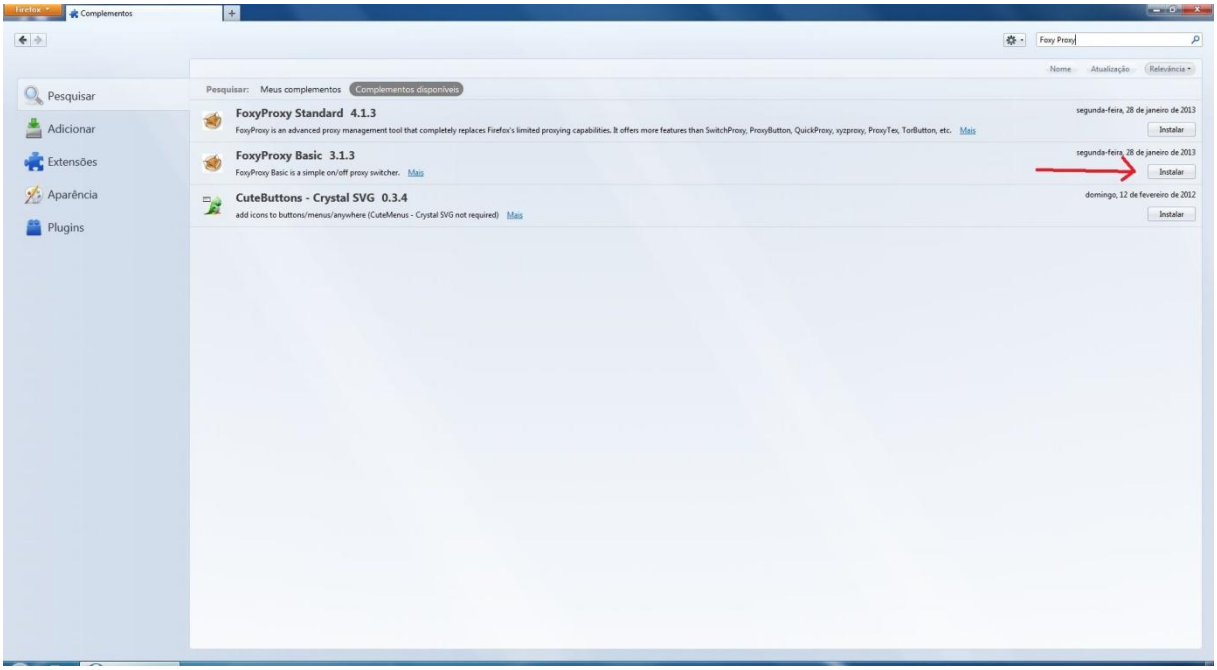


na janela mostrada acima, deveremos clicar em "Adicionar", que fica no topo da coluna de botões que ficam na parte da esquerda da janela.

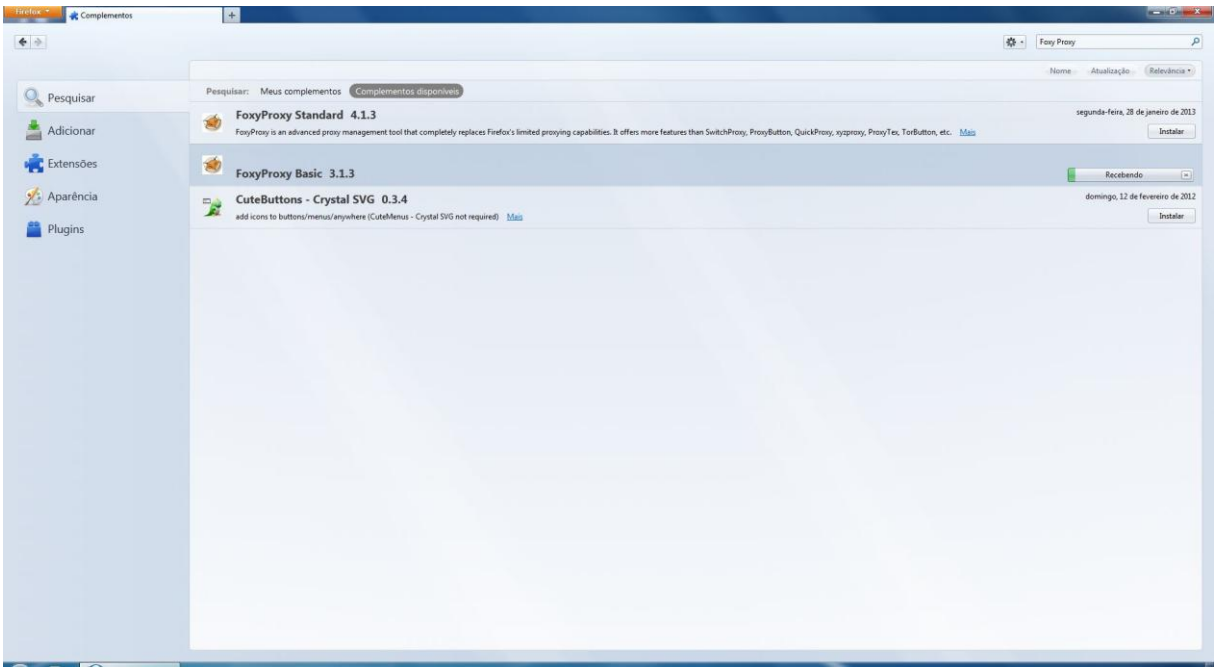
Isso fará com que seja exibido um feed de notícias sobre as novidades em complementos para o Firefox. Nós deveremos digitar "Foxy Proxy" e pressionar ENTER, no campo de busca por complementos que fica no canto superior direito da janela, como mostrado na figura abaixo:



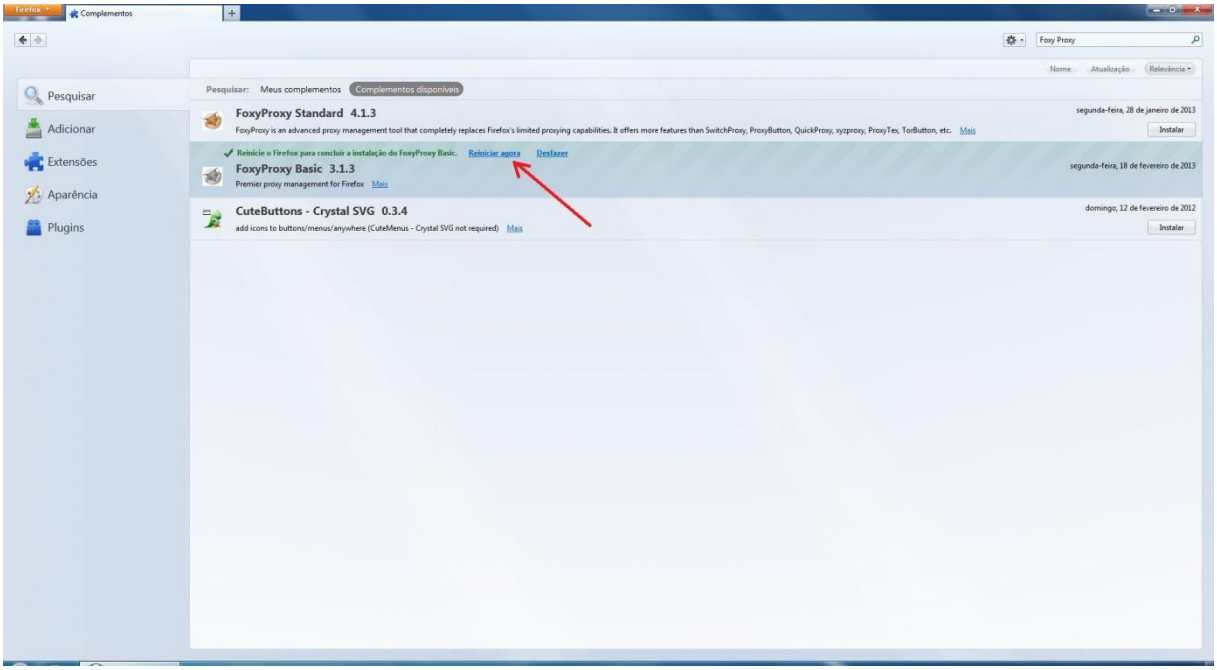
Nos resultados de busca por complementos com o nome que digitamos, deveremos escolher o FoxyProxy Basic (a versão atual enquanto este tutorial é a 3.1.3), e então clicaremos em "Instalar", como é apontado na figura abaixo:



Isso fará com que o processo de instalação do complemento seja iniciado no Firefox, assim:

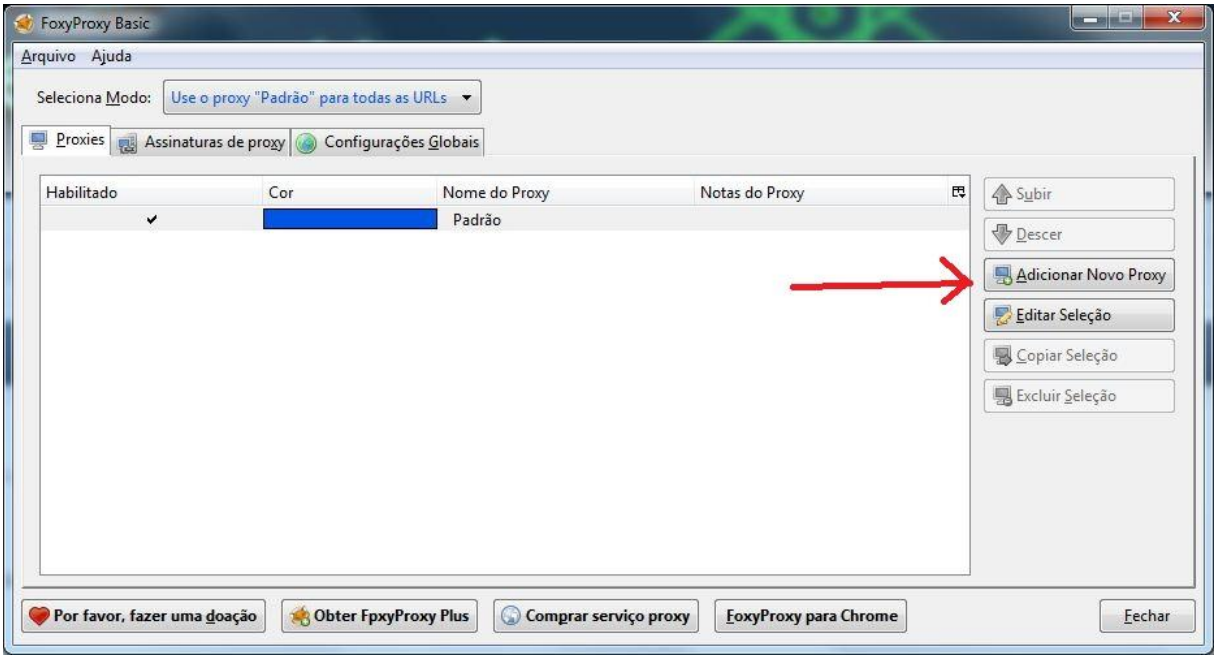


Após terminada a instalação, é necessário reiniciar o Firefox, o que pode ser feito clicando-se no botão mostrado abaixo:

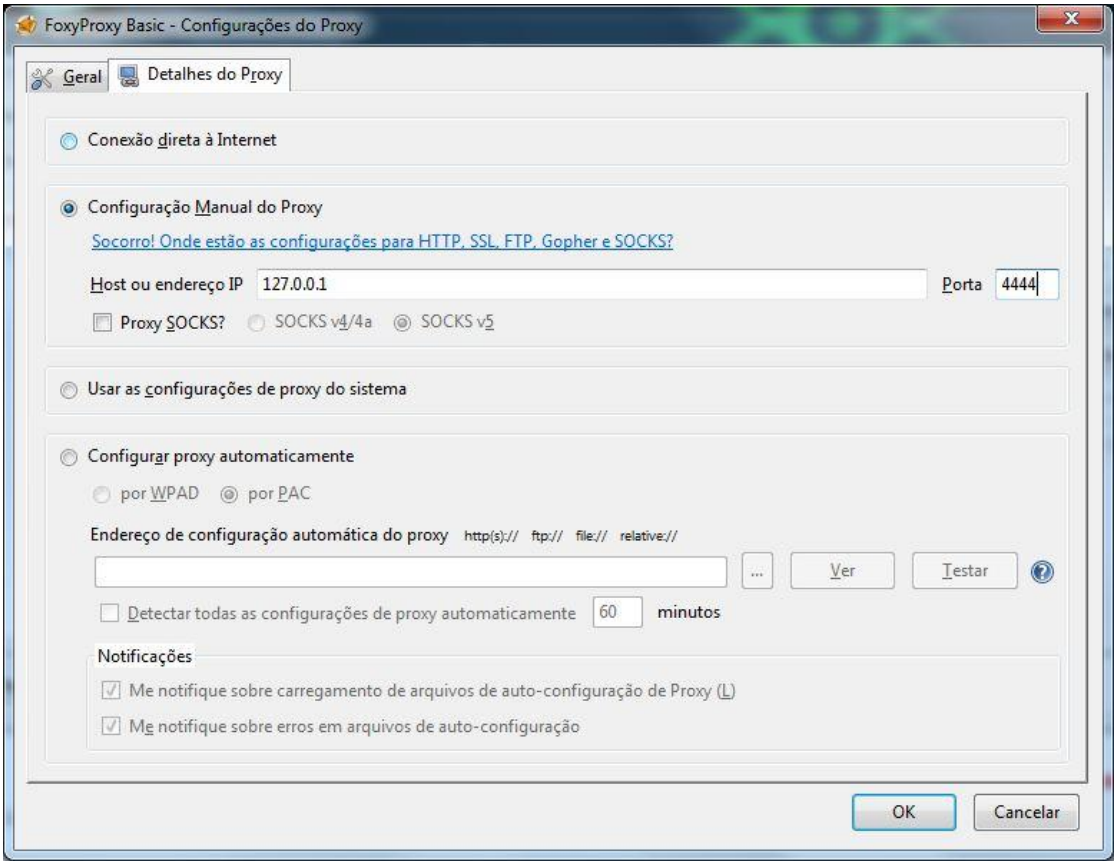


Após reiniciado o Firefox, é interessante que os leitores notem que a partir de agora há o ícone de uma raposa na cor azul junto à barra superior do Firefox, como mostrado na figura abaixo:

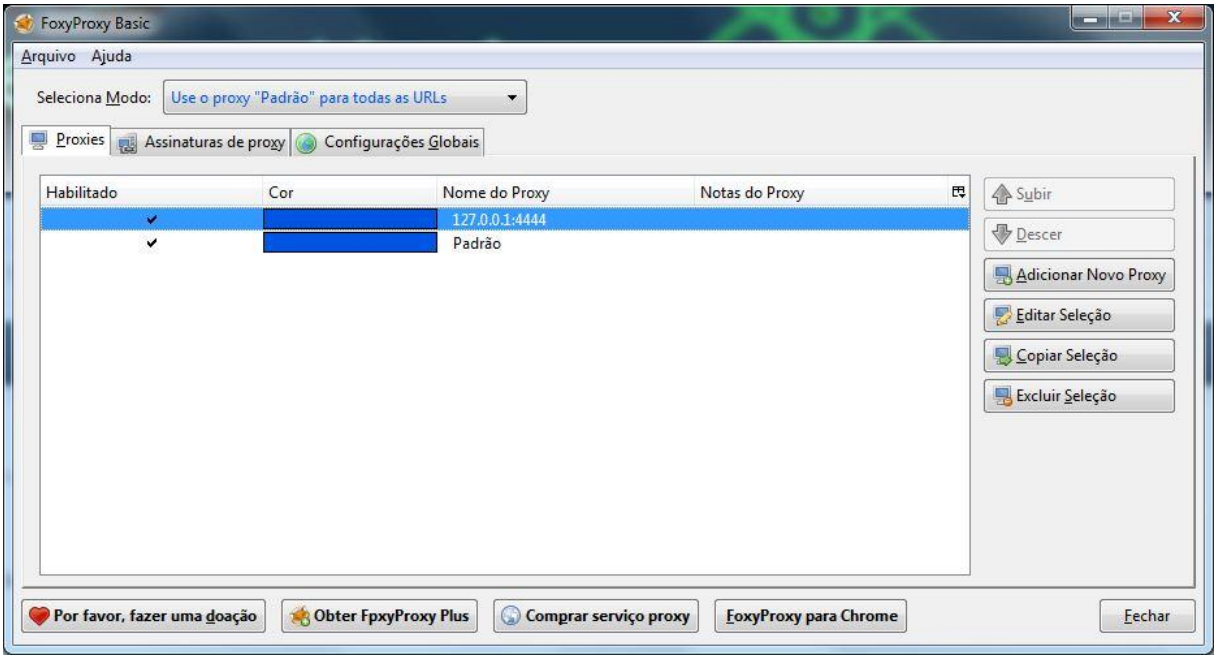
Para configurarmos nossa conexão à rede I2P, deveremos clicar duas vezes no ícone da raposa, e então será exibida a seguinte janela:



Como se vê apontado na imagem acima, devemos clicar em "Adicionar Novo Proxy", e então será aberta a janela de configuração da proxy, que deverá ser deixada como se mostra a seguir:

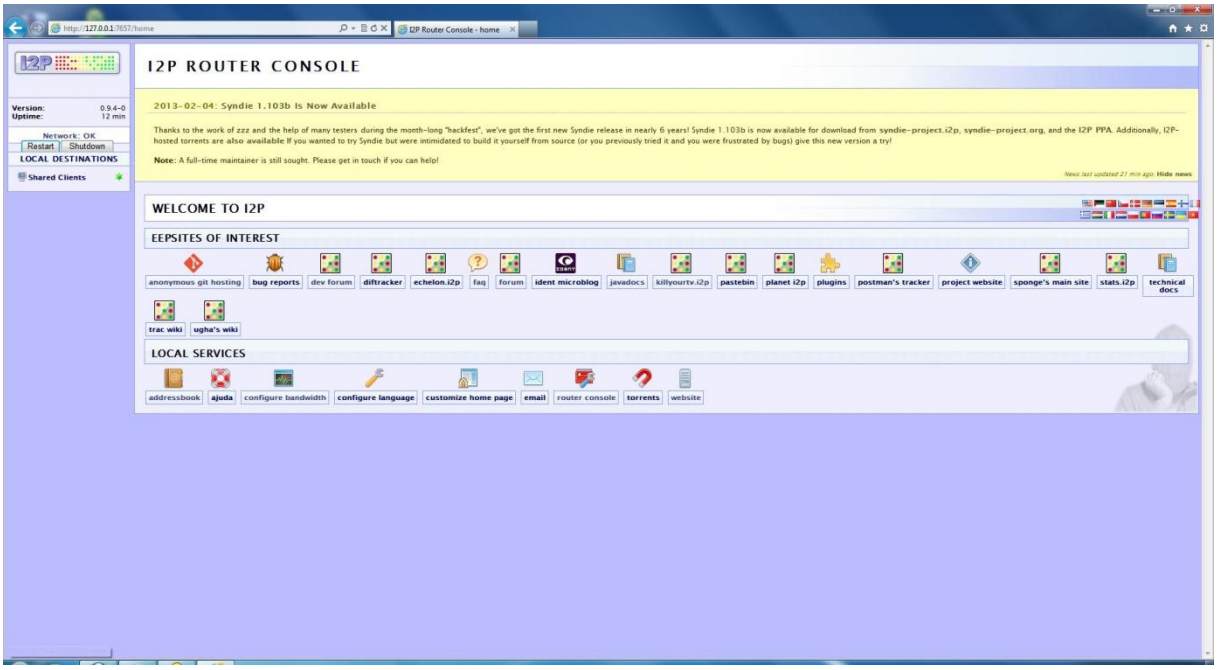


Após clicarmos em OK na janela ilustrada acima, podemos notar que agora a janela do Foxy Proxy ficou assim:



Então já configuramos uma proxy para podermos navegar na rede I2P. Mas ainda precisamos ativá-la. Para isso, clicamos em "Fechar", na janela do Foxy Proxy, e, na janela normal do nosso navegador Firefox, clicamos 1 vez em cima do ícone da raposa azul, e então deixamos seleciona da opção "Use o Proxy 127.0.0.1:4444" para todas as URLs, como é mostrado abaixo:

Agora sim. Fechamos o navagedor Firefox, e então podemos iniciar o programa "I2P Router Console" que foi colocado na nossa área de trabalho. Isso fará com que algum outro navegador que esteja instalado no computador se inicie, porém com a janela principal do console do roteador I2P sendo exibida, assim:

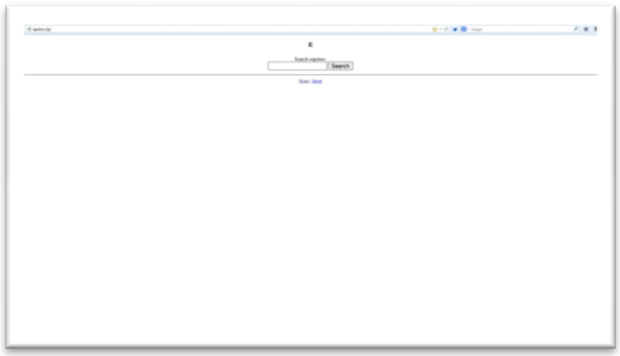


Essa janela do console do roteador I2P deve ser somente minimizada, não fechada, enquanto quisermos navegar na rede I2P. Quando não mais quisermos, aí sim deveremos fechá-la.

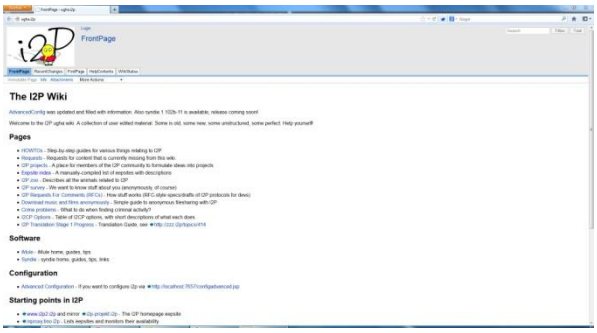
Já com a janela do roteador I2P minimizada, vamos abrir nosso Firefox (pois como configuramos a conexão do I2P para ser feita através dele, é somente nele que poderemos navegar na rede I2P) e então poderemos acessar sites dessa rede criptografada, com tudo funcionando corretamente.

Para finalizar, deixamos abaixo algumas sugestões de sites I2P para os usuários iniciarem suas pesquisas, buscando manter o melhor foco possível no conteúdo desejado:

Epsilon (http://epsilon.i2p/) - Um motor de buscas similar ao Google, porém destinado a exibir somente sites I2P em seus resultados de busca.



Ugha's Wiki (http://ugha.i2p/) - coleção de links para outros sites e artigos de enciclopédia em um formato wiki.



Perv I2P (http://perv.i2p/stats.cgi) - lista sites da rede I2P e avalia sua disponibilidade na rede.

Identity Guy (http://identiguy.i2p/) - lista sites da rede I2P e avalia sua disponibilidade na rede.

Conclusão

Com os procedimentos ensinados ao longo deste tutorial, é possível que usuários menos experientes possam dar seus primeiros passos nas redes Onion e I2P, realizando pesquisas em motores de busca dedicados às suas respectivas redes, e assim aprofundarem seus conhecimentos em qualquer área desejada.

Além disso, com os saberes apontados neste material de estudo, é possível que os usuários novatos possam entrar em contato com ferramentas anônimas de comunicação, bem como com outros grupos Anonymous que se encontram reunidos nas redes Onion e I2P, o que fortalece o engajamento na causa Anonymous e assim cresce numérica e qualitativamente o contingente de ativistas por um mundo mais justo.

Viva Anonymous.

Viva Lacking Faces.

Somos uma legião.