

DEEP WEB E REDES DESCENTRALIZADAS

NATANAEL ANTONIOLI



FÁBRICA DE
NOOBS

Prefácio

Se você veio até aqui, é porque provavelmente tomou conhecimento sobre a Deep Web através de pesquisas na internet, encontrou meu canal e foi direcionado para a leitura dessa apostila. Neste, pretendo esclarecer algumas das dúvidas que o público geral costuma ter sobre o assunto, e lhe dar as primeiras orientações para se iniciar na exploração das redes da Deep Web.

Por alguma razão, a Deep Web é um tema extremamente midiático e sensacionalizado. Em qualquer veículo, seja ele impresso, de televisão ou na internet, são poucas as reportagens sérias sobre o assunto. Essa apostila é uma delas.

Aqui, apresentarei a definição técnica e prática do que é a Deep Web. Esqueça qualquer coisa que você leu sobre camadas, conteúdos secretos, paranormalidade, entre outros. A realidade nesse caso é, felizmente ou infelizmente, um pouco diferente do que é ditado pelo senso comum.

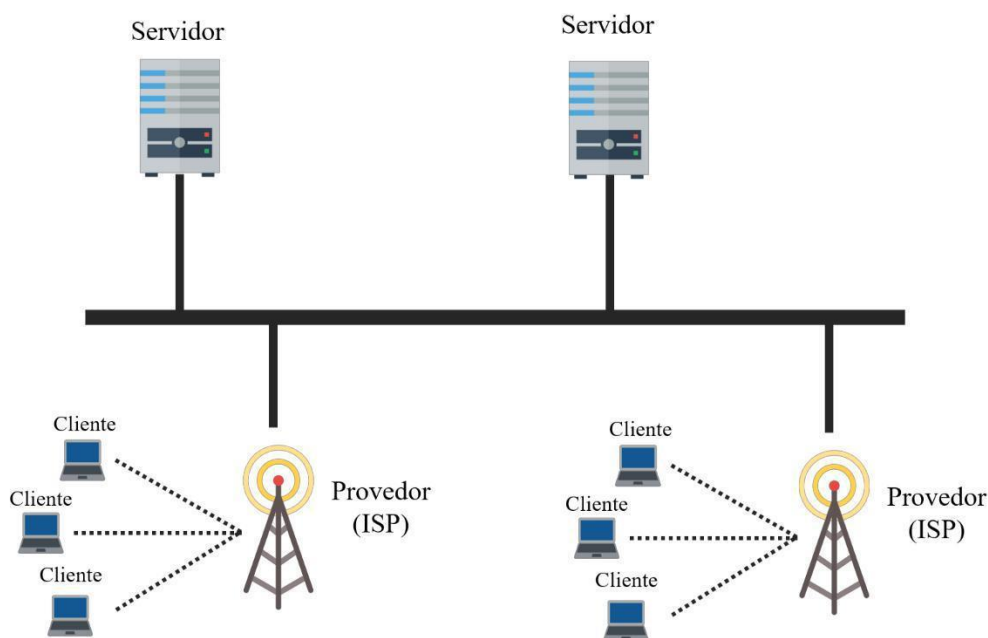
Espero que ela lhe sirva para aprender mais e, quem sabe, se iniciar nesse novo universo. Boa leitura!

Meus sinceros agradecimentos à Mariana Schneider, que realizou a revisão gramatical desta apostila.

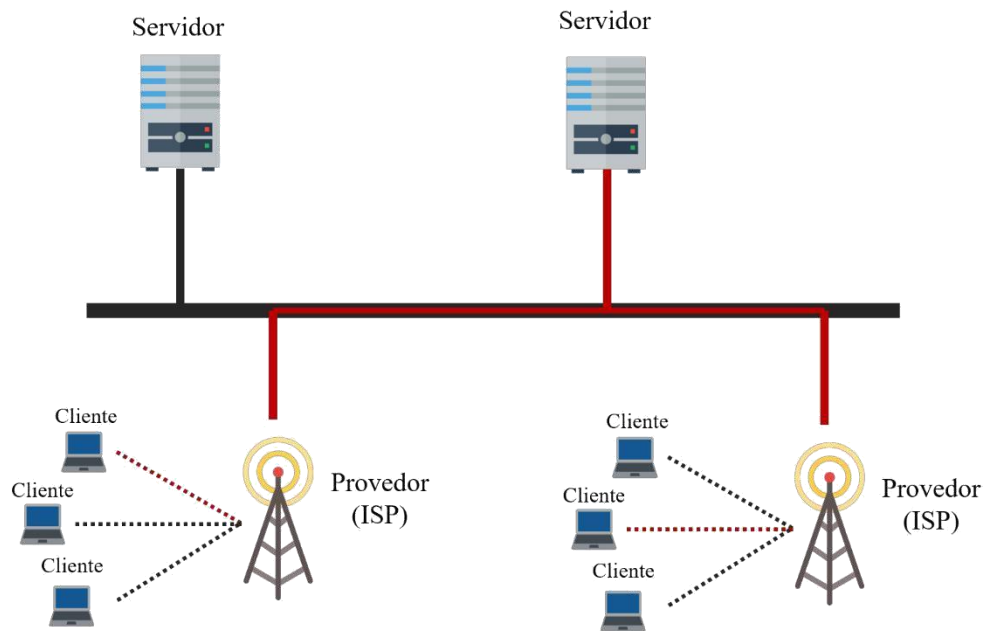
I. Definição Técnica da Deep Web

Antes de definirmos o que é a Deep Web, será necessário definirmos o que é a Internet na qual você está navegando agora. Como talvez já deva saber, a rede mundial de computadores pode ser ilustrada como um fio, interligando diversos equipamentos. Entre eles, os servidores, a partir dos quais sites são armazenados e operados, de forma que tudo que passa por eles é centralizado. Já os computadores (clientes) são conectados a um provedor de internet (ISP), responsável por realizar a conexão entre esses e a rede.

Cada equipamento conectado à rede recebe um número, denominado protocolo de IP, que é usado para identificar o mesmo e garantir que as conexões sejam devidamente realizadas.



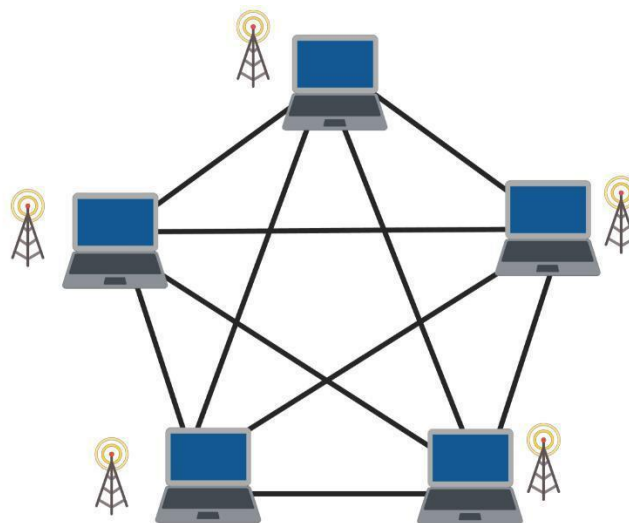
Quando uma conexão é realizada, pacotes de informação são enviados do cliente para o ISP, do ISP para o servidor, e do servidor para seu destino, seja ele o mesmo que enviou a informação ou um computador diferente. No diagrama abaixo, as linhas representam o trajeto percorrido por um e-mail, saindo do cliente, indo para o provedor, e sendo entregue em seu destino.



Perceba que, durante o processo, todo o conteúdo passa por um servidor central. Por consequência, os pacotes de informação podem e vão ser acessados, lidos e provavelmente armazenados nesse servidor. Além do mais, caso o mesmo seja desligado da internet, o serviço fica fora do ar, de forma temporária ou permanente.

Assim, os usuários (ou clientes) tornam-se dependentes de um servidor. É justamente para evitar isso que a Deep Web existe. Através dela, usuários podem se comunicar sem depender de um servidor central, e, na maioria dos casos, de forma anônima.

Mas como isso é possível? A descentralização é dada graças a chamadas redes peer-to-peer (ou P2P). Nelas, cada computador (agora chamado de node), através de seu respectivo provedor, se conecta com outros computadores integrantes da rede, de forma que a transmissão de pacotes é feita diretamente de node para node.



Caso seja necessário armazenar alguma informação (um arquivo compartilhado, por exemplo), esse arquivo é transferido (de forma parcial ou integral) para os demais nodes. Quando um dos nodes que não o possui solicita acesso a ele, ele é “remontado” no seu local de destino a partir das partes armazenadas em cada node. Toda essa infraestrutura é gerenciada por um software, que deve estar presente em cada computador da rede P2P. Cada software corresponde à uma rede P2P.

Através do método acima, livramo-nos de dois problemas: o serviço sempre estará disponível, uma vez que não há um servidor central para ser desligado (salvo em casos onde todos os computadores se desconectam simultaneamente), e informações que dizem respeito a determinados nodes passarão apenas por eles.

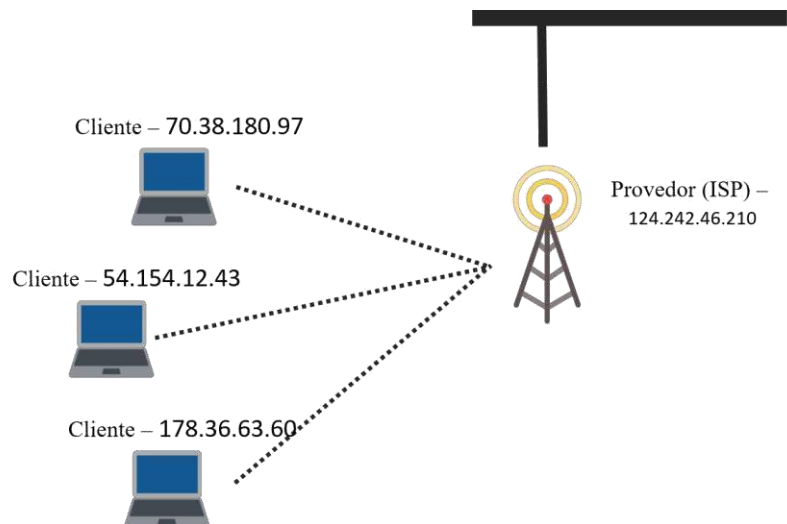
Essa é a base de toda rede da Deep Web. É natural que alguns desses softwares gerenciadores apresentem funcionalidades extras, como encriptação do tráfego, sistema para mascarar o protocolo de IP, código aberto, entre outros. Quanto mais dessas funcionalidades uma rede apresentar, mais “pura” digamos que ela é.

Assim, os principais pilares para uma rede P2P ser classificada como parte da Deep Web são:

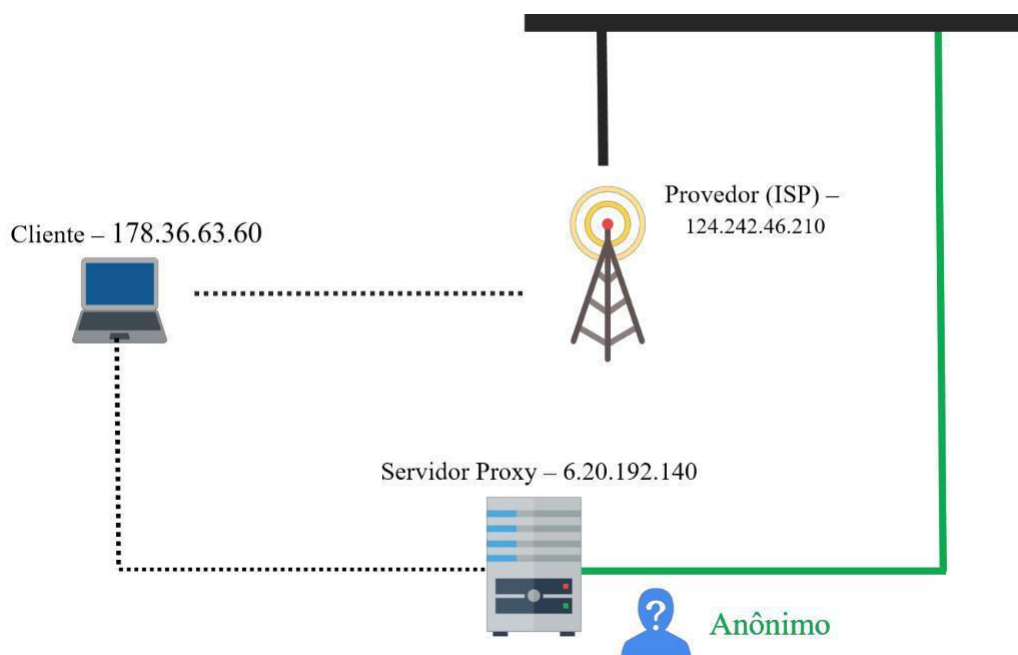
- Descentralização;
- Anonimato;
- Segurança de Pacotes;
- Código Aberto.

Explicarei agora como cada um desses outros 3 quesitos é desenvolvido dentro de uma rede P2P.

Como mencionado acima, cada computador conectado à internet é identificado por um número, denominado IP. A partir de um número de IP, pode-se relacionar diversos pacotes de informação com um mesmo computador, descobrir sua localização e provedor de internet, e, portando uma ordem judicial, descobrir a pessoa responsável por operá-lo. É até mesmo possível realizar ataques de stress, causando transtornos e lentidão à rede.

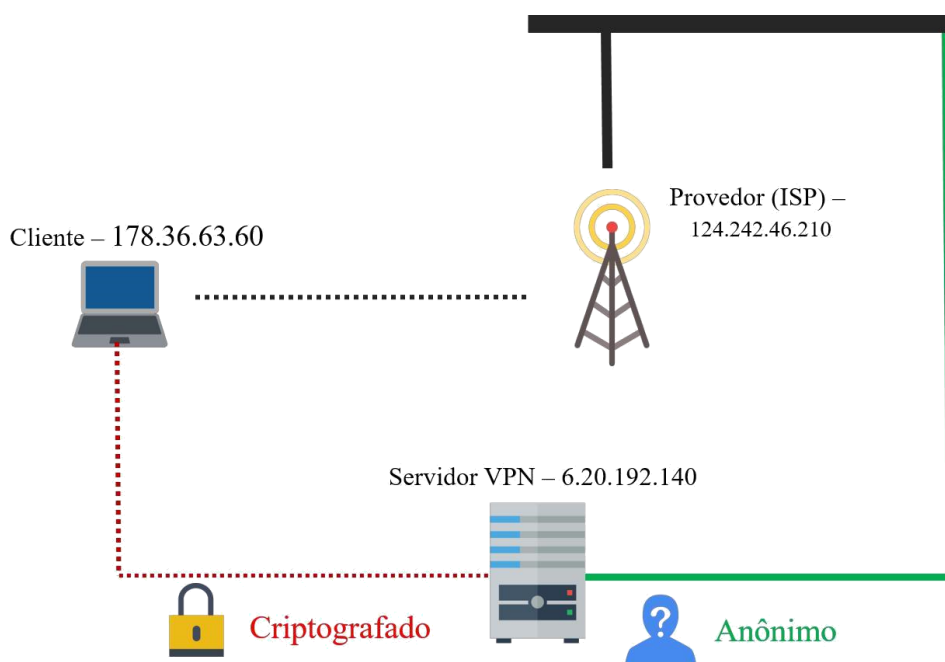


Sendo assim, o anonimato é conquistado através da alteração do endereço de IP original para outro. Isso é feito através de um servidor de proxy. Um proxy é caracterizado por ser um servidor que atua como um intermediário entre o cliente e a internet. Qualquer tráfego percorrido através de um servidor proxy irá parecer ter se originado a partir do endereço IP dele, em vez do seu.



Algumas redes, como a Onion, conseguem fazer com que o servidor de proxy seja descentralizado, inexistindo assim uma máquina central.

Já a segurança dos pacotes é garantida através da encriptação dos mesmos, de forma que um interceptador não consiga decodificá-los. Um sistema capaz de realizar a função é chamado de VPN, e funciona de forma semelhante ao proxy, com a diferença de que uma VPN irá criptografar todo o tráfego de rede entre o cliente e o servidor proxy.



Por fim, possuir um programa de código aberto permite que qualquer usuário possa revisar o código fonte do programa, podendo encontrar vulnerabilidades e se garantir que o mesmo cumpre o que promete.

Alguns programas, como o Tor, apresentam esses quatro requisitos. Outros, como o sistema de Torrents, apenas alguns deles.

Mas o que efetivamente faz parte da Deep Web? Existem diversas classificações. Alguns preferem englobar apenas as redes que apresentem todos os quesitos, enquanto para outros, qualquer rede que apresente um desses já pode ser considerada parte da Deep Web.

Aqui, usarei a segunda classificação. Porém, irei ressaltar que na prática, algumas dessas redes – mesmo sendo, em termos técnicos, parte da Deep Web – são amplamente utilizadas, e por essa razão, não são exatamente consideradas como tal.

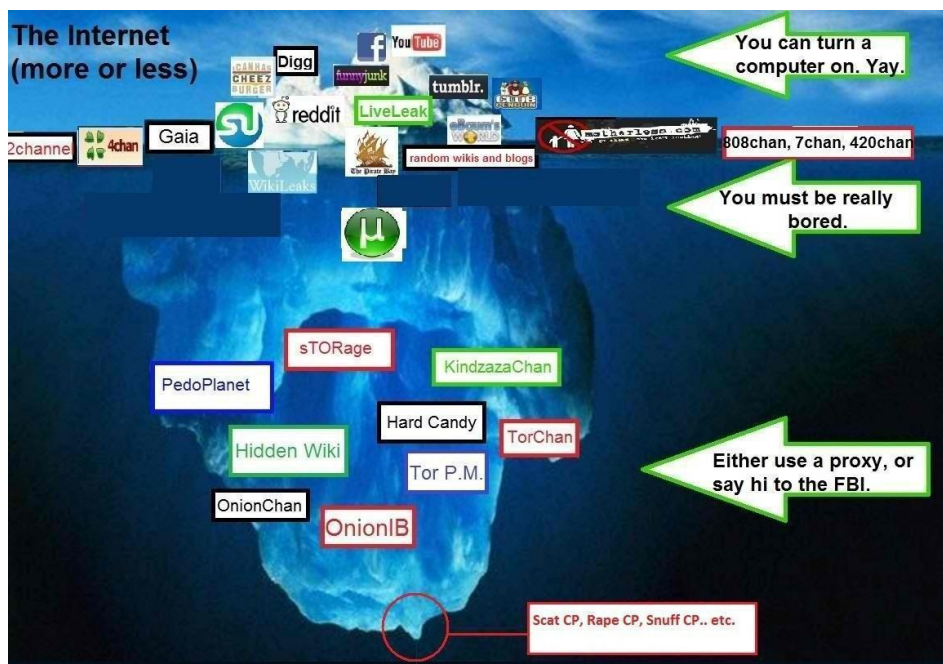
Algumas delas são voltadas para a postagem de sites, outras para o compartilhamento de arquivos, outras para comunicação instantânea, enquanto que uma ampla gama delas permite a estruturação de um sistema monetário, como as Bitcoins.

II. Como a Deep Web “funciona”?

Provavelmente você já leu ou assistiu em algum lugar que a Deep Web é dividida em camadas, tendo níveis que aumentam de profundidade conforme tipo de conteúdo postado ou dificuldade de acesso.

Tal definição é falsa por dois motivos: a Deep Web é composta por redes distintas e independentes entre si. Logo, é impossível classificá-las em numerais ordinais, e muito menos em níveis. Além disso, qualquer conteúdo pode ser postado em qualquer lugar, e dificuldade de acesso é um conceito relativo.

Logo, a tão famosa imagem do iceberg não faz sentido algum.



Que tipo de conteúdo posso encontrar na Deep Web? Como mencionado, uma rede da Deep Web – principalmente as mais populares – possui, além da descentralização, forte anonimato. Isso significa que algo postado por lá não poderá ter seu autor rastreado, exceto em situações de falha humana (as quais serão apontadas no decorrer desta apostila).

Logo, qualquer conteúdo que necessite de tal anonimato será encontrado em muito maior proporção na Deep Web do que na internet comum. Isso inclui, em sua maioria, atividades ilegais, como comércio de produtos ilícitos e pornografia ilegal. Além disso, pessoas que vivem em situação de repressão podem se valer do anonimato para realizar denúncias e se comunicar sem risco de serem presas ou executadas.

A Deep Web também pode ser uma vasta fonte de conhecimento, através de bibliotecas – nas quais material é compartilhado sem restrições autorais – e de fóruns que permitem discussões irrestritas. Não é incomum encontrarmos também

materiais que não haveriam necessidade alguma de serem postados lá, como brincadeiras e episódios de My Little Pony (sim!).

Segue uma lista de conteúdos com maior probabilidade de serem encontrados lá.

- Tráfico de drogas e armas;
- Venda de produtos variados, geralmente ilegais; Tutoriais hackers;
- Provedores de e-mails anônimos;
- Fóruns de variedades, nos quais pessoas que não querem ser identificadas participam;
- Portais de notícias que geralmente são censurados;
- Vazamento de documentos e informações;
- Sites comerciais de pornografia legal e ilegal;
- Pessoas com gostos um pouco estranhos contando sobre eles; Crimes financeiros;
- Bancos de dados;
- Bibliotecas;
- Download de conteúdos piratas;
- Supostos** arquivos de OVNI's e outras coisas paranormais;
- Enigmas;

É importante destacar que algo de cunho paranormal encontrado lá não se difere do mesmo conteúdo encontrado na internet comum. Não é porque veio da Deep Web, que isso significa que ele seja verdadeiro ou tenha origem sobrenatural.

Em contrapartida, a Deep Web não é um oráculo. Você não terá acesso a milhões de informações sobre tudo, muito menos conseguirá entrar em bancos de dados de governos ou universidades e nem visualizar provas de concursos com antecedência. Tais bancos de dados são protegidos de outras formas, que não têm relação alguma com as redes da Deep Web.

Considere que, para um conteúdo ser postado na Deep Web, é preciso que alguém o poste. Se você procura por algo extremamente específico (já me pediram link para baixar o filme dos Trapalhões na Deep Web) dificilmente terá sucesso em achar simplesmente porque ninguém o postou. Nessas situações, é infinitamente mais viável procurá-lo no Google.

Por ser uma língua internacional, a maioria dos conteúdos encontrados em qualquer rede estará em Inglês. Terá de se acostumar caso pretenda navegar.

Aproveitarei para comentar a ideia de que a Deep Web é um lugar perigoso. Para te convencer do contrário, usarei um encadeamento lógico.

As principais redes da Deep Web têm, por característica, o anonimato e a segurança. Logo, pessoas as usam para atividades ilegais. Elas só fazem isso por estarem seguras, por estarem livres de qualquer responsabilidade pelo que postam – inclusive por parte de agentes policiais.

Logo, você também estará. O programa garante essa segurança, o que privilegia tanto criminosos, quanto pessoas dentro da legalidade. Assim, você não será alvo de hackers. A chance de isso acontecer somente navegando em uma rede da Deep Web tende a zero.

Existem criminosos e agentes policiais na Deep Web, mas a não ser que você dê motivos, ninguém irá fazer nada contra você, simplesmente porque ninguém consegue determinar quem você é.

Para um hacker,^[5.2] dar motivos seria fazer downloads sem tomar algumas medidas de segurança antes. Para um agente policial, praticar qualquer atividade ilícita. Se você não cometer crimes, pode ficar tranquilo em relação aos policiais, e se você se proteger, não há o que temer em relação a criminosos.

Além disso, a maioria das redes de compartilhamento de sites já contam com VPN. É impossível acessá-las sem camuflar seu endereço de IP. Logo, você não será “rastreado”, como adoram dizer.

Existe a possibilidade de você acidentalmente cair em um site que preferia não ver, assim como aconteceria na internet comum. Nesse caso, basta sair dele.

Se todos esses anos de navegação na internet não lhe traumatizaram, garanto que não será um site visto de relance que o fará. Além do mais, você só encontrará (e verá por um tempo maior que alguns segundos) tais conteúdos se realmente os procurar. Por experiência própria, digo que já vi muito mais coisas que preferia não ver scrollando meu feed no Facebook do que navegando na Deep Web.

Sem contar que a maioria das “fotos da Deep Web” que se encontra ao pesquisar o termo, vieram de vários lugares, menos da Deep Web. Assista a este vídeo <https://youtu.be/Wbgb3lgMluA> caso queira saber mais.

Falaremos agora sobre motores de busca. Antes disso, irei lhe propor um exercício, a fim de facilitar a explicação.

Imagine a internet comum e a Deep Web como dois universos. São incrivelmente grandes, com um número imenso de corpos celestes (galáxias, estrelas, planetas etc.). O número de elementos que há nesses universos só não é maior que uma coisa: o espaço vazio que também há neles.

Agora, imagine que na internet comum pode-se viajar para qualquer lugar desse universo sem maiores problemas. Logo, o espaço vazio deixa de importar,

afinal, ele não atrapalha em nada. Isso representa as engines de busca, como o Google.

Já na Deep Web não há como chegar em qualquer lugar com tanta facilidade. Logo, é impossível conhecer tudo o que existe nela, uma vez que a probabilidade de encontrar um espaço vazio é infinitamente maior que a de encontrar algum conteúdo. Existem engines que chegam perto disso, mas ainda não se comparam ao poder das que temos na Surface.

É aí que entra a parte de mitologia virtual. Por ser um espaço desconhecido, qualquer um está livre para fazer as suposições que desejar, mas são apenas suposições. Justamente por isso, existe tanta especulação sobre o tema.

Por essa razão, a melhor forma de encontrar conteúdos na Deep Web é através de diretórios de links:^[6.1] sites que postam links atualizados frequentemente. É necessária alguma sorte para encontrar o que procura com facilidade. Outra opção também é pedir por indicações de links em fóruns e comunidades voltadas ao assunto.

Além disso, recomendo acompanhar essa playlist <https://youtu.be/g1KUu0pWmnc?list=PLIevgZoV2cAh1qICQoYNH9hkWk4tgc yjM>, na qual posto, mensalmente, novos links em diversas redes da Deep Web.

III. Medidas de Segurança

É perfeitamente natural que todo usuário se mostre um tanto receoso antes de adentrar na Deep Web. Porém, com algumas dicas simples de navegação, você dificilmente correrá riscos.

As recomendações a seguir são voltadas para a rede Onion, mas também servem como genéricas para qualquer outra rede, e algumas, também para a internet comum.

De início, saiba que uma rede já é programada para que as devidas medidas de segurança sejam tomadas pelo próprio programa. Por exemplo, o Tor camufla o IP do usuário, a Freenet criptografa as páginas armazenadas em seu computador, e assim por diante. Sendo assim, nenhum programa adicional é necessário, basta uma mudança de hábito.

A navegação em páginas (sem interação) também costuma ser segura. É impossível a execução de qualquer script em páginas acessadas sem a permissão do usuário, ainda mais navegando-se pelo Tor.

Vários usuários têm dúvida sobre o uso de JavaScript nas páginas. O JavaScript é uma ferramenta fundamental para navegação em alguns sites, mas inútil em outros – em especial aqueles feitos em HTML puro, maioria na DeepWeb. Porém, seu uso pode apresentar vulnerabilidades, permitindo o rastreamento do usuário.

Garanto, por experiência própria, que a não ser que esteja exercendo alguma atividade que exija anonimato, não há problemas em mantê-lo ativado, assim como outros plug-ins. Há casos recentes de uma vulnerabilidade no Adobe Flash Player. Recomendo a mesma procedência.

Além disso, alguns programas apresentam configurações que permitem selecionar o nível de anonimato. Elas podem abranger detalhes como nodes com os quais seu computador se conecta, plug-ins habilitados, entre outros. Se você não precisa de maior anonimato, recomendo manter as configurações padrão.

Apesar da navegação ser quase sempre anônima e segura, a partir do momento em que um arquivo é baixado, ele passa a se localizar na máquina. Desse ponto em diante, o anonimato propiciado pela rede não é mais suficiente, uma vez que, a partir de seu desligamento, o arquivo ainda está lá, e, caso contiver algum código malicioso, pode permitir o rastreamento e causar danos às vítimas.

De início, digo para evitar terminantemente o download de qualquer arquivo cuja posse seja ilegal, como pornografia infantil, uma vez que, ao fazer o download, estará cometendo um crime e pode ser responsabilizado pelo ato.

Quanto a outros arquivos, os riscos que corre ao baixá-los são exatamente os mesmos que você já está acostumado a correr na internet comum.

A não ser que o arquivo em questão contenha um trojan, não existem riscos em sua posse. Sendo assim, antes de realizar um download, recomendo investigar sua procedência. Eis algumas instruções:

O domínio onde ele está hospedado possui boa reputação? Um exemplo de serviço com boa reputação são bibliotecas conhecidas. Um exemplo oposto disso é um programa multiplicador de Bitcoins que você encontrou enquanto navegava por um diretório de links.

É um arquivo de posse ilegal? Não baixe. Além de cometer um crime, vários arquivos do tipo são postados como armadilhas para capturar criminosos. Se é um tutorial sobre falsificar impressões digitais, por exemplo, a simples posse do arquivo não tem nenhuma implicação legal. Nesse caso, passe para as outras regras.

Qual a extensão do arquivo? Normalmente, arquivos como imagens, vídeos ou livros são menos propensos a conter ameaças. Evite os executáveis, entradas de registro, dll's e outras extensões destinadas a arquivos do sistema. Caso encontre uma extensão desconhecida, pesquise sobre ela.

Após realizar o download, uma eventual infecção por trojan só ocorreria após o arquivo ser executado. Sendo assim, aproveite para testá-lo em scanners de vírus.

Caso ainda esteja receoso, pode abri-lo em uma máquina virtual ou sandbox. Essas duas ferramentas restringem a execução do arquivo para um ambiente controlado, evitando modificações na máquina original.

Você pode aprender mais sobre técnicas de navegação segura aplicáveis não somente na Deep Web em <https://youtu.be/8zVsR495F-M>.

Quando se procura participar de comunidades, frequentemente o usuário depara com sites que exigem algum tipo de cadastro, normalmente fornecendo algumas informações.

Não recomendo expor informações verdadeiras em comunidades na Deep Web. Isso por que, caso a comunidade em questão esteja envolvida com um tópico ilegal e seja tomada por agentes policiaes, seus dados estarão associados com ela – e não por que hackers podem pegar suas informações e usar elas contra você, isso não acontece.

Sendo assim, use apelidos, dados falsos e o que mais for necessário para resguardar sua privacidade, afinal o anonimato depende também do usuário. Quanto aos endereços de e-mail, recomendo utilizar um e-mail temporário (criado preferencialmente com o uso de uma VPN) ou um totalmente anônimo (operável somente a partir do Tor ou outra VPN). Você pode aprender sobre esses dois tópicos, respectivamente, em <https://youtu.be/2WXbAhn56SY> e <https://youtu.be/DqPqMHpmK3A>.

Outro tema recorrente é a questão de compras. A Deep Web é também conhecida pelos diversos mercados virtuais onde todo tipo de mercadoria é vendida. Não é necessário relevar que não recomendo a compra de nenhum item ilegal.

Porém, com exceção de restrições alfandegárias e impostos, não há problemas na compra de outros tipos de itens. Entretanto, há algumas coisas que você deve saber.

Não há a quem recorrer caso uma compra na Deep Web não ocorra conforme suas expectativas. Sendo assim, tais negociações jamais terão o mesmo nível de confiabilidade existente em sites como o Mercado Livre.

Logo, a única forma de diferenciar um golpe de uma negociação séria é através da reputação do site vendedor. Para tanto, pergunte sobre ele em diversos fóruns, e procure por usuários que já realizaram compras lá. Analise o feedback recebido e decida com base nessas informações.

A forma de entrega da mercadoria varia. Alguns sites possuem sua área de atuação restrita à uma região, outros despacham a mercadoria pelo correio e outros usam serviços terceirizados de entrega. Todos esses detalhes devem ser informados no site em questão.

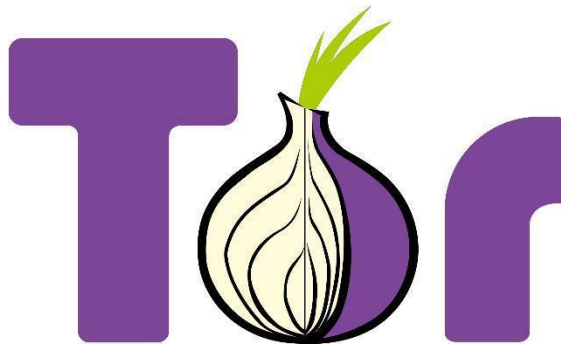
Além disso, a transação comercial provavelmente será feita através de criptomoedas, mais especificamente, Bitcoins. Sendo assim, você precisará antes se familiarizar com essa forma de negociação. Recomendo estudar sobre o assunto em <https://www.youtube.com/watch?v=Ydsqv8mysBc>.

IV.Redes Populares

Agora que a maioria das questões quanto ao funcionamento da Deep Web já foram esclarecidas, iremos, brevemente, estudar algumas das principais redes da Deep Web e outras não tão populares, mas curiosas.

Ressalto que existem centenas de redes na Deep Web, atualmente aproximaria para algo entre 400 projetos distintos, alguns maiores, outros menores. Por essa razão, é inviável mencionarmos algo maior que 5% delas nessa apostila. Parte do meu trabalho envolve a documentação detalhada de cada uma dessas redes. Você pode conhecê-lo e se informar melhor sobre redes de seu interesse, além de aprender o passo a passo para acessá-las e navegar nelas em <http://fabricadenoobs.wixsite.com/home/redes-da-deep-web> e <https://www.youtube.com/watch?v=WQLxfgbmeUQ&list=PLIevgZoV2cAgMYes2vNpoChDsKXPzxGTM>.

Sem dúvidas, a Onion é a rede mais popular da Deep Web, e é muitas vezes confundida com toda a Deep Web. Acessada a partir do navegador Tor, a rede funciona de forma descentralizada, e possui uma VPN integrada.



Essa VPN, ao contrário das demais, não possui um único servidor, mas sim vários servidores descentralizados, chamados de routers. Ao estabelecer uma conexão, alguns desses routers, em média 6, são escolhidos aleatoriamente e usados para direcioná-la. Assim, é impossível realizar o caminho de volta e encontrar o IP original. Além disso, em cada router, uma nova camada de encriptação é adicionada.

Tal característica permite que o Tor não sirva somente para acessar a rede Onion, mas também navegar anonimamente pela internet convencional, tornando-o ferramenta fundamental para quem busca anonimato.

Dentro da rede, sites podem ser encontrados em diretórios de links, sendo os mais conhecidos o Harry 71 (<http://skunksworke2cg.onion/>), o OnionDir (<http://auutwvpt2zktxwng.onion/>), o Parazite (<http://kpynyvym6xqi7wz2.onion/links.html>), e a HiddenWiki (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page).

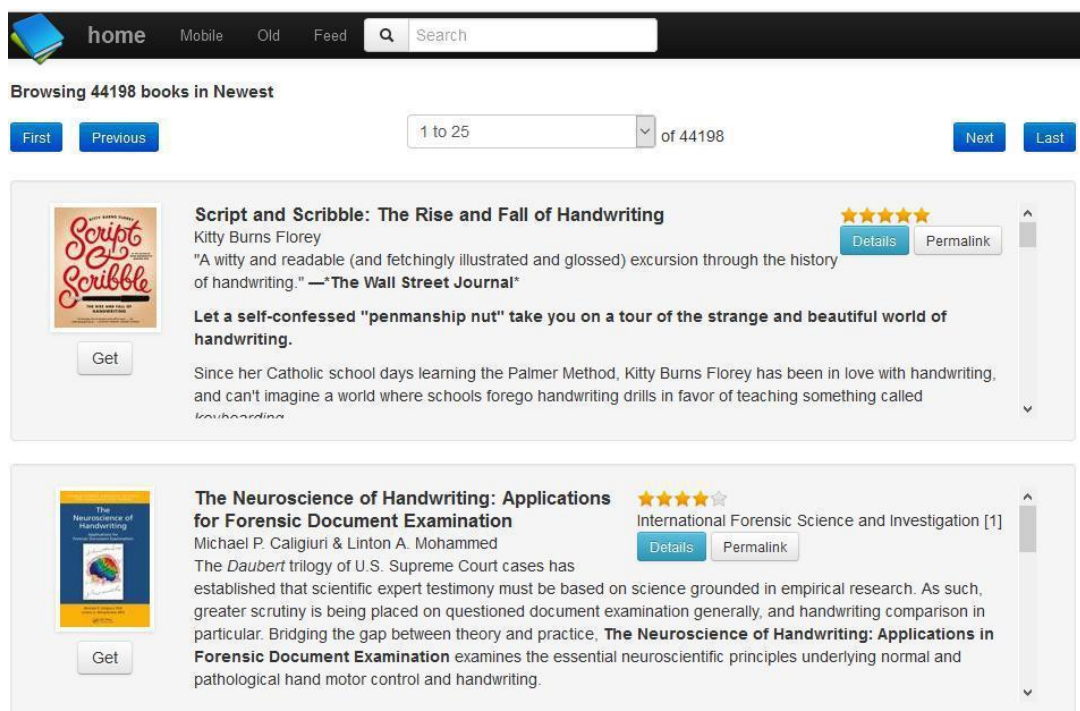
Vale lembrar que eles saem do ar com frequência, então é comum se deparar com erros indicando que não é possível acessar determinado site.

Abaixo, a HiddenWiki, espécie de enciclopédia do conteúdo na rede Onion.



The screenshot shows the 'Main Page' of The Hidden Wiki. The page has a navigation sidebar on the left with links for 'Main page', 'Recent changes', 'Random page', and 'Rules of the site'. Below this is a search bar and a 'tools' section with links like 'What links here', 'Related changes', 'Special pages', 'Printable version', 'Permanent link', and 'Page information'. The main content area includes tabs for 'main page', 'discussion', 'view source', and 'history'. The 'Main Page' title is followed by a welcome message and a new hidden wiki URL. Below this is an 'Editor's picks' section with a list of five articles, including 'The Matrix', 'How to Exit the Matrix', 'Verifying PGP signatures', 'In Praise Of Hawala', and 'Terrific Strategies To Apply A Social media Marketing Approach'. A 'Volunteer' section follows, listing six tasks such as 'Plunder other hidden service lists for links' and 'File the SnapBBSIndex links'. The page ends with an 'Introduction Points' section.

Em seguida, a Calibre, biblioteca que agrega mais de 40 mil títulos, sendo acessível em <http://clockwise3rldkgu.onion/libr/>.



The screenshot displays the Calibre library interface. At the top, there's a navigation bar with 'home', 'Mobile', 'Old', 'Feed', and a search bar. Below this, it says 'Browsing 44198 books in Newest'. A pagination bar shows '1 to 25 of 44198' with 'First', 'Previous', 'Next', and 'Last' buttons. The main content area lists two books. The first book is 'Script and Scribble: The Rise and Fall of Handwriting' by Kitty Burns Florey, with a 5-star rating and a 'Details' button. The second book is 'The Neuroscience of Handwriting: Applications for Forensic Document Examination' by Michael P. Caligiuri & Linton A. Mohammed, with a 4.5-star rating and a 'Details' button. Both books have a 'Get' button next to their covers.

Demonstrando o lado criminoso da Deep Web, temos um site que vende informações vazadas (<http://cmarketsuhtiix5.onion/>), como bancos de dados sobre pessoas, modelos para documentos falsos, entre outros.

CMARKET
INTERNATIONAL CRIMINAL MARKETPLACE

WELCOME CRIMINAL MARKET | Advanced Persistent Threat | Cyberspionage

Personal Information
Sale of personal information , contains all the information people a complete whole country from their home to their identity number , Sales of this information are millions of people that contains GB compressed information .

Government Documents
Editable documents of very high warm in original documents with valid stamps Original products , Everything is original of government efficiency in Fraud

Government Identification
Many will identifications that are sold on the internet these identifications are original , from its system templates with random record number

Energy Information
Energy systems along with their personal database system includes different information from different countries , the size of these files are GB of information

NEWS PRODUCTS | NEWS ATTACK
NATION INFORMATION
CYBERSPIONAGE
APT ATTACKS
ENERGY INFORMATION
HEALTHCARE
GOVERNMENT ATTACKS
APT | ZERO
SCADA SYSTEM
TARGET ATTACK 0
BANK ATTACKS
INT - SYSTEM
0 DAY ATTACK PLATAFORM
MANAGEMENT SISTEMS
COMPANY ATTACKS

E também um torturador por encomenda oferecendo seus serviços em <http://idomquol7lannf22.onion/>.

The Mechanic

This site contains No JavaScript, No Cookies, No 3rd party code.

Do you have a problem that needs to be "fixed"?

Is there a person out there you want to have "fixed"?

If so we can help you

The Mechanic has over 10 years experience in ensuring that troublesome people are no longer an issue

What makes us different from other similar services?

- No age restrictions - we provide service to people from newborns to the elderly

- No choice in methodology - Unlike other services that provide "extended suffering" and other such options. When you hire us you have no choice in what methods are used. We will maximize the likelihood of a successful hit and escape from law enforcement

- We are not cheap - If you are looking to have this service done on the cheap. Don't bother contacting us. The final price will vary depending on various factors

- We are not quick - Many other services state that they provide a extremely fast turnaround on their contracts. We take the time to figure out the best way to perform the operation in a clean manner. We are not thugs with guns who fire aimlessly and hope we hit the target.

- Willing to travel worldwide - Of course the cost of airfares and accommodation will be factored in to the price. As well as the price of acquiring new "tools" at the destination. Don't stay at budget hotels

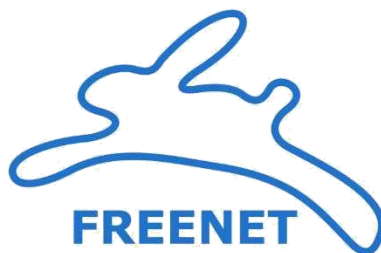
Proof of work

Unlike other sites we are willing to provide a photograph from a previous job to show that we mean business

Click on the link below to see the image

Com algumas configurações, qualquer pessoa pode hospedar um site na Onion e rodá-lo a partir de seu próprio computador. Porém, ele só funcionará enquanto a máquina usada na hospedagem estiver ligada e com o Tor iniciado.

Em paralelo, temos a Freenet, uma rede também descentralizada voltada à publicação de sites anônimos, destinada principalmente a driblar censuras impostas por governos.



A rede não apresenta navegador próprio, e é acessada a partir de um programa de mesmo nome capaz de configurar qualquer navegador – incluindo o Tor – para acessar a Freenet.

É exigido do usuário que ele destine uma parte de tamanho flexível de seu disco rígido para o armazenamento de conteúdos hospedados na rede, o que a torna mais estável se comparada à Onion.

Além disso, existem também várias configurações de segurança personalizáveis para cada necessidade.

Alguns dos principais diretórios de links são o Enzo Index (<http://localhost:8888/USK@XJZAi25dd5y7lrxE3cHMmM-xZ-c-hlPpKLYeLC0YG5I,8XTbR1bd9RBXIX6j-OZNednsJ8Cl6EAeBBebC3jtMFU,AQACAAE/index/711/>) e o Nerdageddon (<http://localhost:8888/USK@tiYrPDh~fDeH5V7NZjpp~QuubaHwgks88iwlRX XLLWA,yboLMwX1dChz8fWKjmbdtl38HR5uiCOdIUT86ohUyRg,AQACAAE/nerdageddon/239/>), exibido abaixo.

LINKAGEDDON
Bookmark Me!

LINKALOG
Read Me

NERDAGEDDON
Generated: 2016-11-05

LINKALOG
Read Me

LINKAGEDDON
Bookmark

Welcome to Nerdageddon. Here we aim to bring you a list of all freesites, both old and new, which could be interesting to political nerds. The links presented here come from [Linkageddon](#) and [Enzo's Index](#), but without the ones flagged as porn and without sites I perceive as boring. Sites are excluded via a blacklist, so new sites will appear here until I remove them to ensure that the index stays useful (though a bit messy) even if I do not get to check the sites.

If you feel the title and/or description for a particular freesite does not give sufficient warning about it's content then please feel free to comment to that effect on [Some](#) or to the relevant FMS board. Note: I promise to filter however I want. If you disagree with my decisions, make your own *geddon. My manual filters are in [checked.json](#).

To make your own *geddon, get [nerd.py](#), [checked.json](#), [template.html](#), [site-styles.css](#), [textlist-styles.css](#) and [activelink.png](#), put them into a folder and run `python3 nerd.py`. Then upload `site/`.

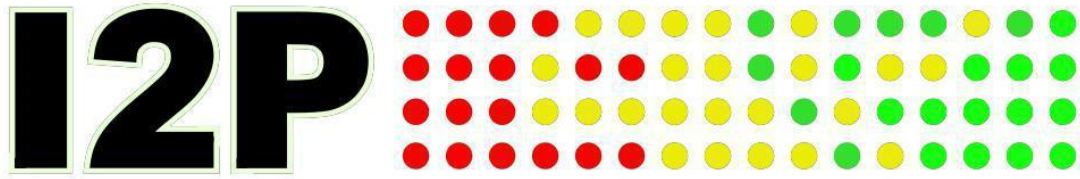
Some bad stuff crept in during the transition to using Enzo's index. I hope that is fixed. If not: please complain! Thanks to Enzo for investigating!

My heuristic filter killed >5% of legitimate sites. It is fixed now. Thanks to anonymous for catching that!

| | | |
|--|--|--|
| Biblioteca Calibre Biblioteca de eBooks en Castellano Added: 2016-06-19 | lawiki2p La Wiki2P, la mayor wiki de las redes invisibles Updated: 2016-06-13 | SiteToolPlugin Added: 2016-06-14 |
| Salvation by Faith, not by Works The Circuit Riding Preacher on the doctrine of salvation by faith Added: 2016-06-14 | FAQ Freesite For Freenet Frosters Added: 2016-06-14 | Freenet News Important News about freenet Added: 2016-06-14 |
| YAFI - Yet Another Freenet Index YAFI is generated by unrestricted crawling of Freenet. May contain very offensive content! Updated: 2016-06-14 | Path to Enlightenment A page on enlightenment Updated: 2016-06-12 | Memorias del Fuego Updated: 2016-06-12 |
| The bad practice in FOSS projects management Julien Danjou Added: 2016-06-10 | Caper Servus Ténébres et lumière : le freesite de Lazare Added: 2016-06-10 | FAQ Freesite For Freenet Frosters Added: 2016-06-10 |
| GNU IceCat | Hillary Duff Tribute A page with Hillary Duff Wallpapers Updated: 2016-06-09 | GNU Coding Standards GNU Coding Standards Added: 2016-06-06 |
| | | Front Page |

Completando a lista de redes mais populares, ainda temos a I2P. Ela possui funcionamento semelhante ao da Freenet: [\[13.4\]](#) também necessita de um software para

acesso e requer ainda algumas configurações adicionais, a fim de redirecionar o tráfego de rede para determinados servidores.




A rede também possui criptografia, constituída, ao todo, por 4 camadas, de maneira parecida com a existente na Onion.

Links podem ser encontrados em sites como o I2P Planet (<http://planet.i2p/>), mostrado abaixo, e o Eepstatus (<http://identiguy.i2p/>), os quais possuem funcionamento semelhante aos demais diretórios já conhecidos.

I2P Planet - The latest around the world of I2P

Tuesday November 29, 2016

Postman Tracker



Open.Range.Weites.Land.mpg

by hidden on Tuesday November 29 at 20:16

<http://www.moviepilot.de/movies/open-range-weites-land> Duration: 02:08:21.91, start: 0.500000, bitrate: 3175 kb/s Stream #0:0[0x80]: Audio: ac3, 48000 Hz, 5.1(side), fltp, 384 kb/s Stream #0:1[0x1e0]: Video: mpeg2video (Main), yuv420p(tv, top first), 720x576 [SAR 64:45 DAR 16:9], 25 fps, 25 tbr, 90k tbn, 50 tbc

Enclosure: <http://tracker2.postman.i2p/index.php?action=Download&id=40187>

Length: 3057305600 bytes

Der.Staatsfeind.Nr.1.mpg

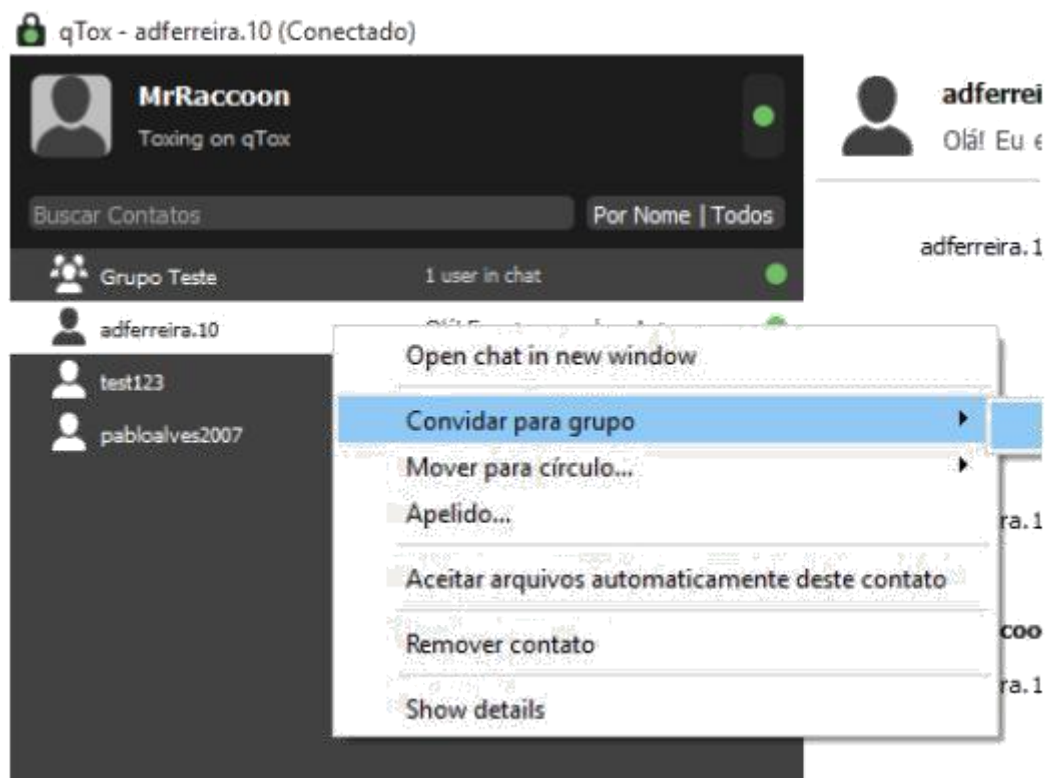
by hidden on Tuesday November 29 at 20:13

<http://www.moviepilot.de/movies/der-staatsfeind-nr-1> Duration: 02:11:51.47, start: 37895.798822, bitrate: 3389 kb/s Stream #0:0[0x1e0]: Video: mpeg2video (Main), yuv420p(tv, top first), 720x576 [SAR 64:45 DAR 16:9], 25 fps, 25 tbr, 90k tbn, 50 tbc Stream #0:1[0x1c0]: Audio: mp2, 48000 Hz, stereo, s16p, 192 kb/s

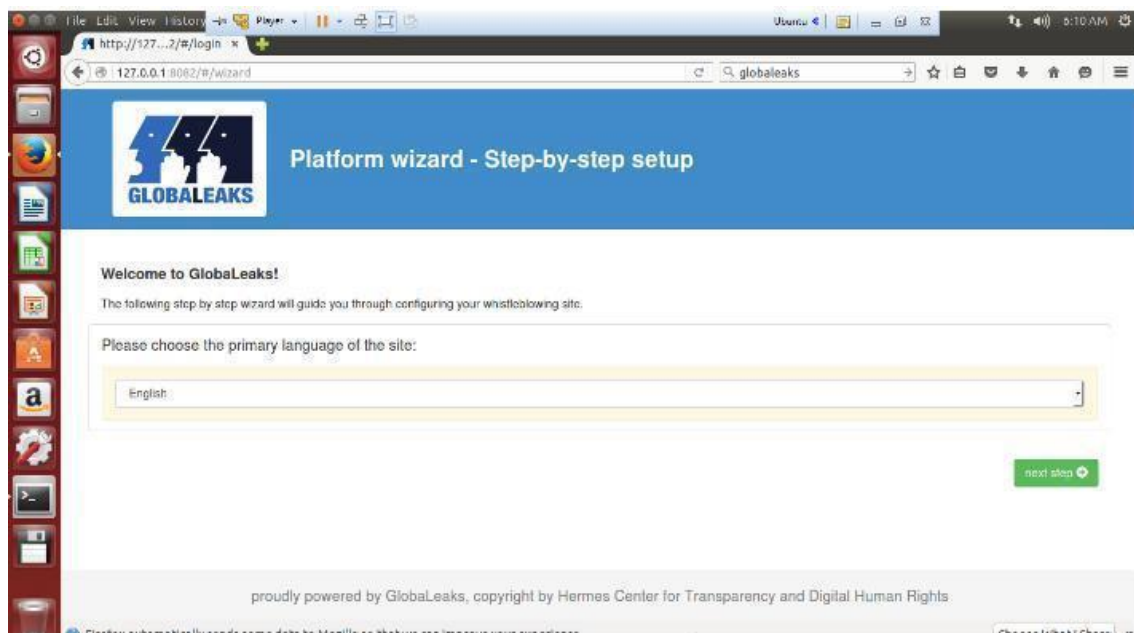
Além dessas redes, existe mais uma infinidade de projetos com diferentes funções. Alguns possuem pouquíssimo conteúdo, outros não possuem código aberto e são gerenciados por uma empresa, enquanto que outros têm tão poucos usuários que podem ser considerados “mortos”. Eis alguns que merecem destaque.

O Tox é uma rede voltada para a comunicação anônima e encriptada. Totalmente de código aberto e multiplataforma, é o tipo de programa que você usaria caso precisasse tratar de algo secreto com alguém.

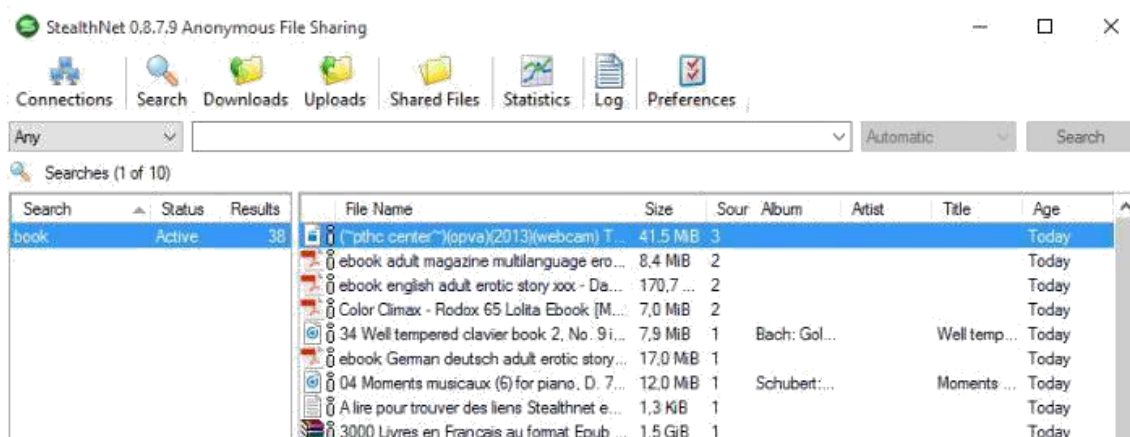
Existem ferramentas para vídeo chamadas, criação de grupos, envio de arquivos, entre muitas outras funções.



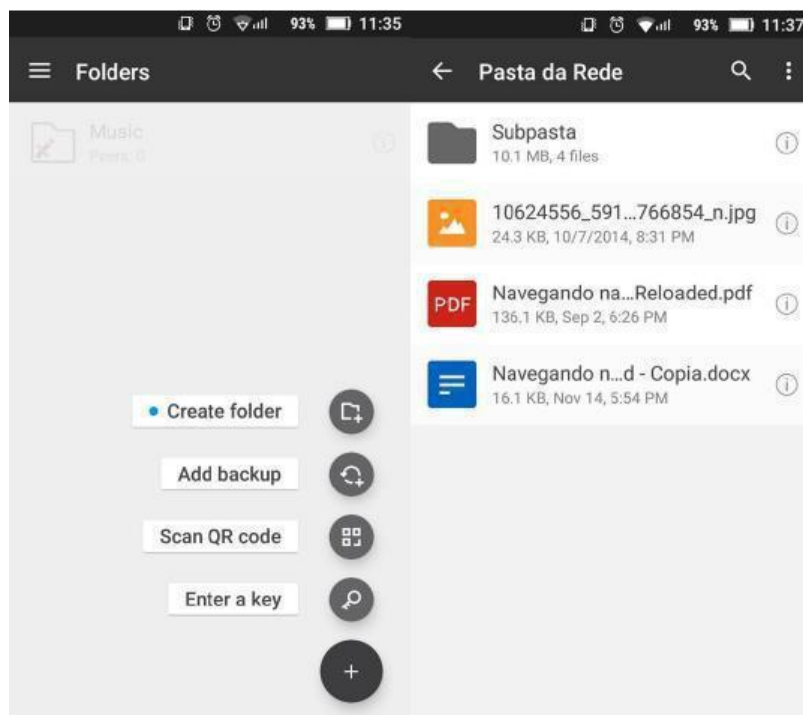
Já a rede Globaleaks é inteiramente baseada em Linux e tem como função a criação de sites para servir de fontes de denúncias, onde informantes podem realizar denúncias anônimas a serem coletadas por jornalistas.



Outra rede interessante é a StealthNet, voltada ao compartilhamento de arquivos e que permite a postagem anônima de qualquer tipo de conteúdo, bem como seu acesso.



Por fim, existem redes feitas para fins comerciais, como a Resilio, que permite a criação de outras pequenas redes, todas com criptografia de ponta a ponta e descentralização, conforme garantido por seu fornecedor.



Pois bem, espero que essa apostila tenha lhe sido útil para esclarecer dúvidas sobre o tema. Seja bem-vindo(a) a esse novo universo. Boa exploração!

