Experimentos com Tor

1. Antes de começar: preparando o ambiente

Primeiro, você precisa fazer o download do Tor Browser e instalá-lo no seu computador. O aplicativo está disponível em https://www.torproject.org/projects/torbrowser.html.en. Este experimento foi feito com a versão 8.0.4, exceto pelo uso da versão 8.5.4 na seção 5. Embora seja possível que a versão atual do navegador seja diferente, é improvável que isso prejudique o entendimento dos experimentos aqui apresentados.

2. Iniciando o aplicativo

Ao executar o aplicativo, você já pode ver algumas informações interessantes na própria tela de inicialização (veja Figura 1). Por exemplo, a mensagem "*Requesting relay information*"("requisitando informação de encaminhamento") representa o primeiro passo do protocolo Tor discutido em aula: a obtenção de nós executando Tor e que, portanto, podem ajudar a aleatorizar o roteamento. Já a mensagem "*Establishing Tor circuit*" ("estabelecendo circuito Tor") indica que o navegador está estabelecendo as chaves com alguns dos nós encontrados, efetivamente criando o circuito de aleatorização.

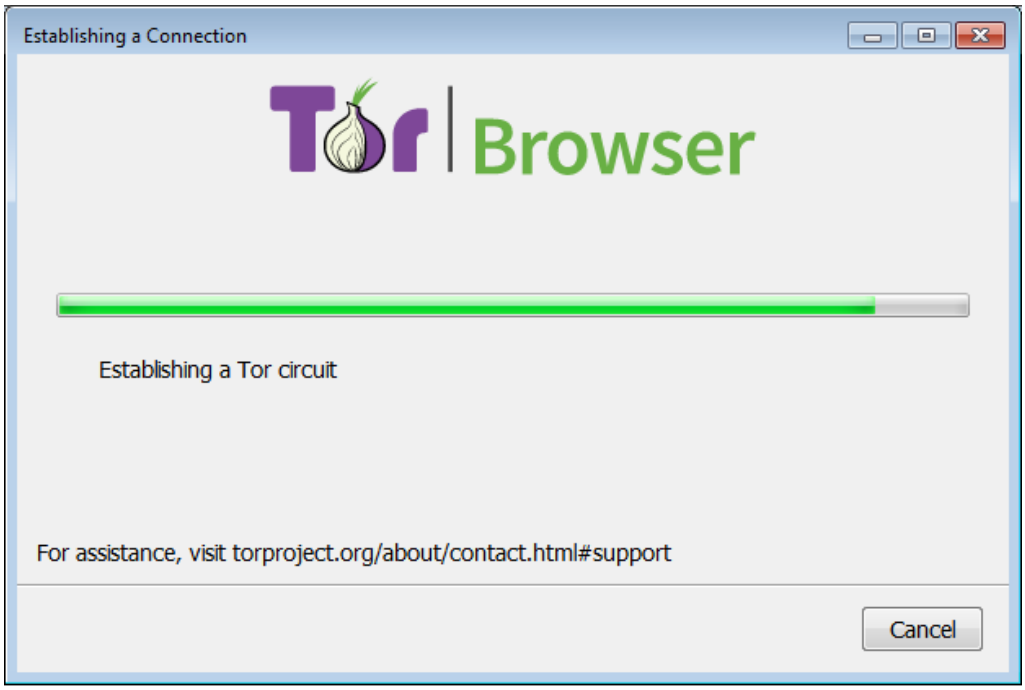

Figura 1 - Inicializando o Tor Browser

3. Navegando sem privacidade

Para verificar um dos principais potenciais das redes Tor, vamos visitar um site que mostra claramente as informações que ele coleta dos usuários visitantes. Um exemplo é o site https://www.localizaip.com.br/ . Esse site mostra o IP do seu computador conforme recebido nas requisições feitas pelo navegador, e então usa essa informação para descobrir a sua localização geográfica.

Comece acessando esse site com um navegador comum, como Opera, Chrome ou Firefox. O resultado deve ser semelhante ao mostrado na Figura 2: o IP público do seu computador (ou do seu roteador, se você estiver em uma rede com NAT – *Network Address Translation*) é mostrado. O sistema também fornece com alguma precisão sua localização geográfica, usando informações públicas sobre onde os IPs são registrados e eventualmente informações extras fornecidas pelo seu computador (e.g., as redes Wi-Fi próximas ao seu computador podem ajudar a revelar sua localização com mais precisão[1]).

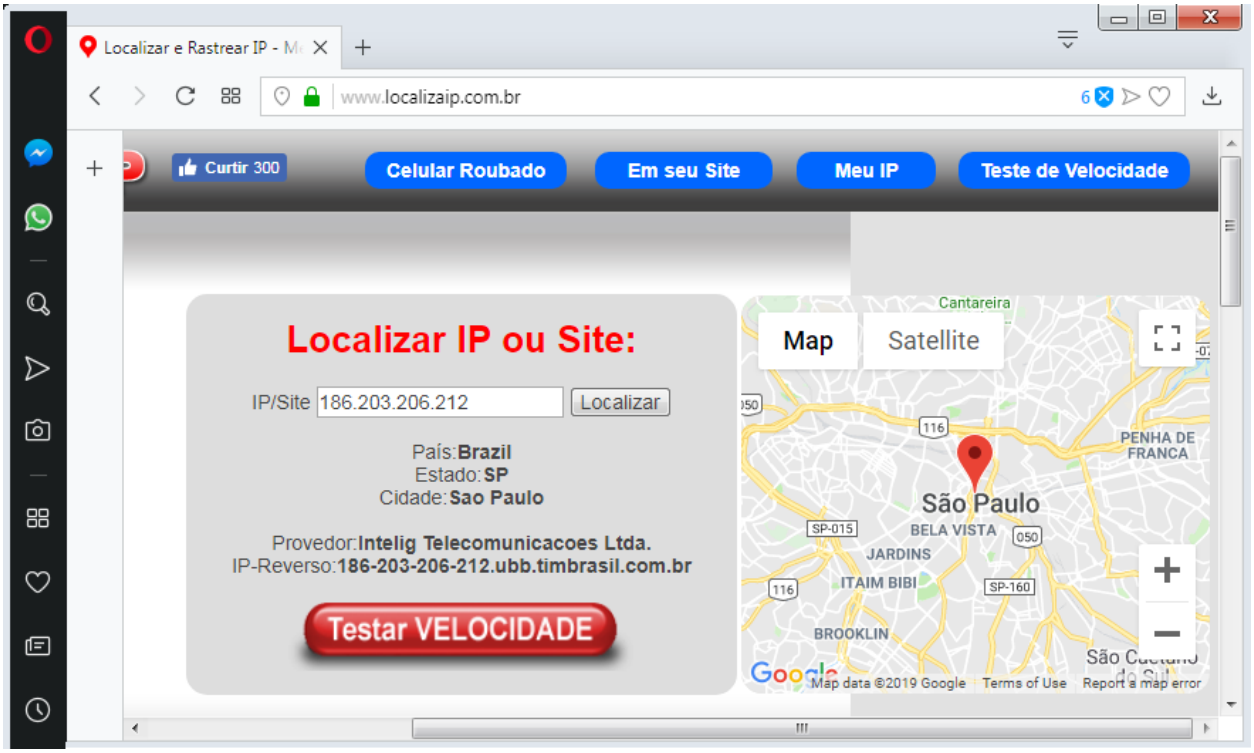

Figura 2 – Navegação com Opera em site que mostra o IP e localização do navegador

[1] https://www.terra.com.br/noticias/tecnologia/internet/google-sabe-a-localizacao-do-seu-roteador-wi-fi-diz-jornal,6938ad6ec72ea310VgnCLD200000bbcceb0aRCRD.html

4. Navegando com privacidade

Repita o experimento anterior usando o mesmo computador, mas em vez de um navegador normal use o Tor Browser: ao acessar a página https://www.localizaip.com.br/, o site deve informar um endereço IP e geolocalização diferentes do verdadeiro. Por exemplo, na Figura 3 o IP mostrado é o de algum computador na Alemanha, embora tenha sido usado exatamente o mesmo computador do experimento realizado na Seção 3, localizado em São Paulo.

Figura 3 - Navegação com Tor Browser em site que mostra o IP e localização do navegador

A razão para essa diferença é bem simples: quem está efetivamente acessando o site é de fato um computador na Alemanha, que também está executando o Tor e que encaminhou seu pedido de acesso para o site. Isso pode ser observado ao clicar no ícone de informação (o pequeno "i") que aparece logo à esquerda do endereço visitado. O resultado deve ser algo similar ao mostrado na Figura 4: essa figura mostra que toda a comunicação com o site passa primeiro pelos EUA (IP 174.141.200.41), depois por um computador na Alemanha (IP 77.21.239.107) e em seguida por outro computador na Alemanha (IP

87.118.92.43), que finalmente envia o pedido ao site visitado. Não por acaso, o IP desse último computador é o único enxergado pelo site visitado.

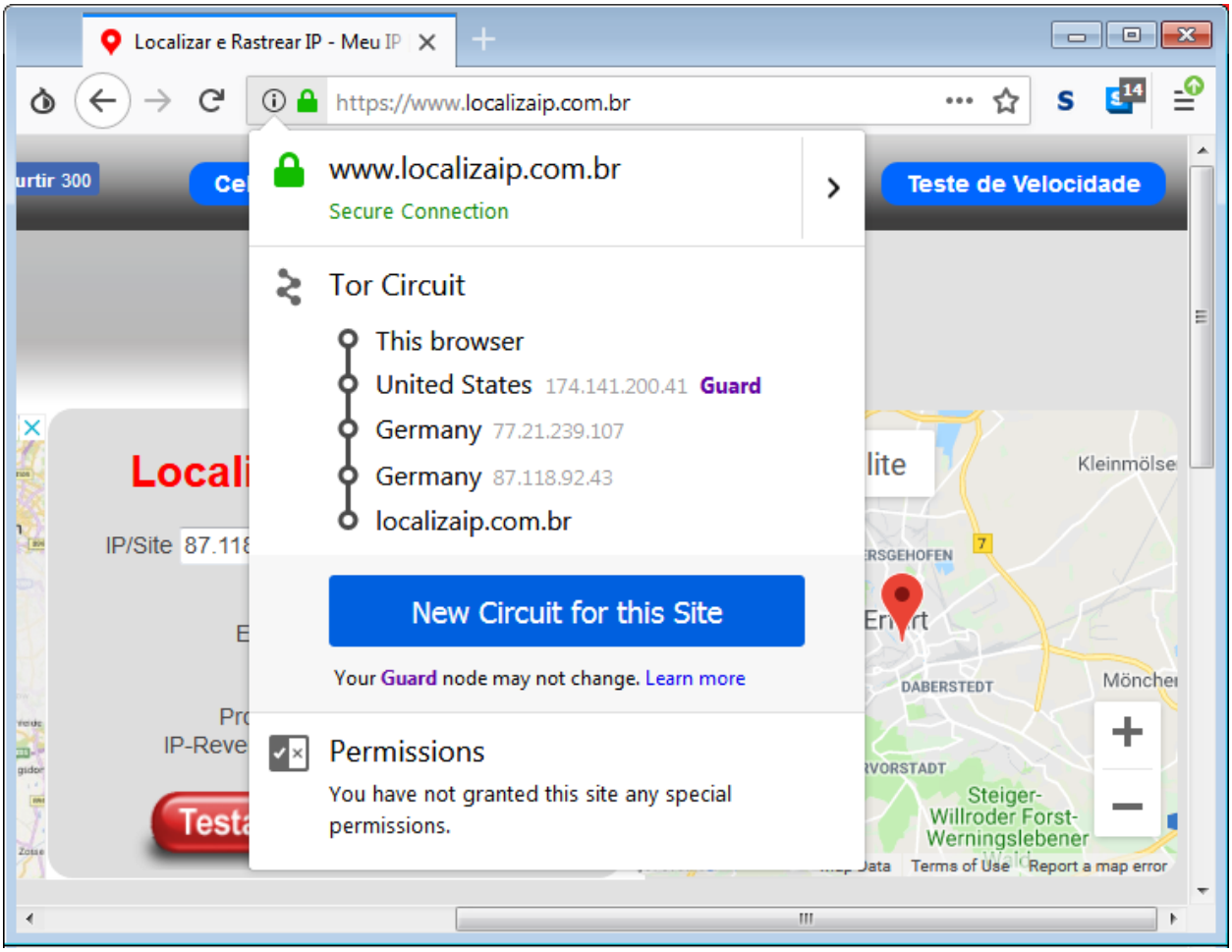

Figura 4 - Navegação com Tor Browser: nós que estão participando da *onion route* ("rota cebola")

Conforme discutido no material da semana 3, esse efeito é observado em qualquer site: sua navegação na Internet pode ser feita enquanto você não revela seu endereço IP aos sites visitados. Isso pode trazer alguns efeitos inusitados, em especial quando você visita sites que ajustam a língua com base na sua localização geográfica. A Figura 5 ilustra esse efeito para o caso do Google, um site que faz esse tipo de ajuste. Perceba que o site foi inteiramente traduzido para a língua do país de onde o Google acredita que está vindo a requisição (no caso, a Suécia, conforme mostrado na Figura 6).

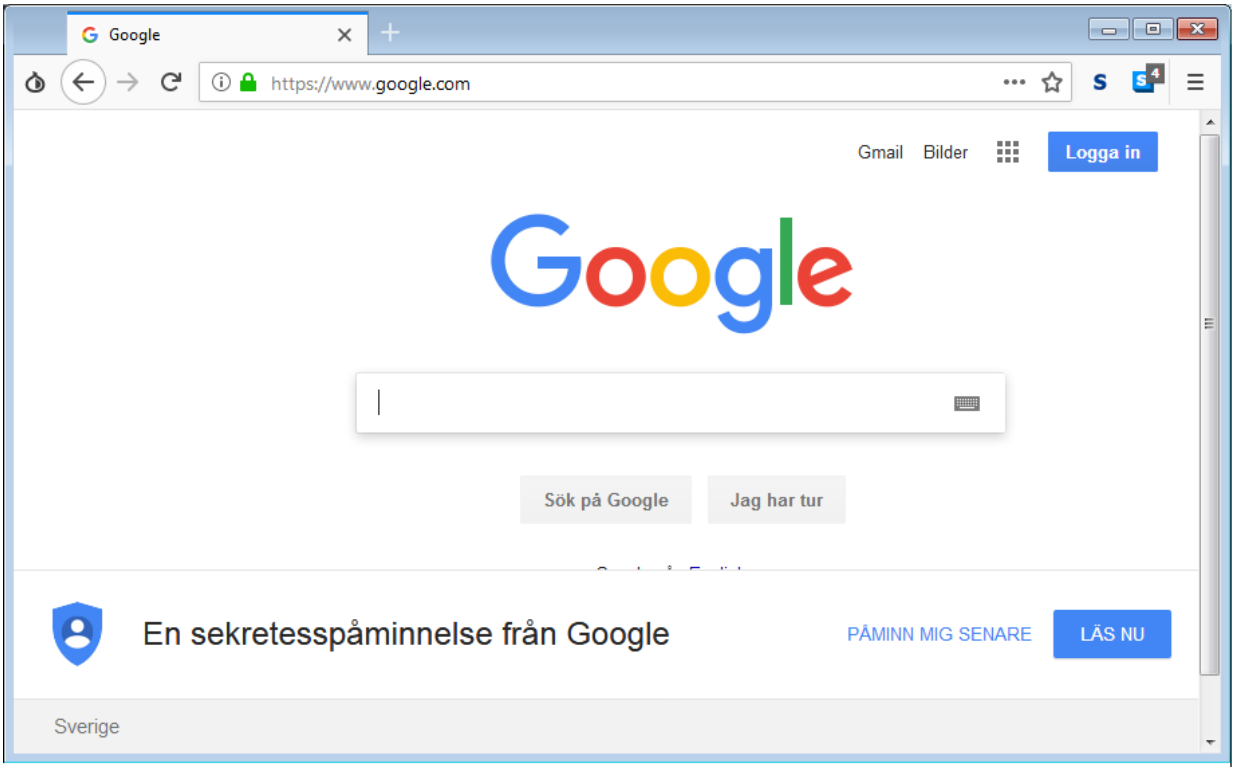

Figura 5 – Acessando o Google a partir da Suécia, via Tor Browser

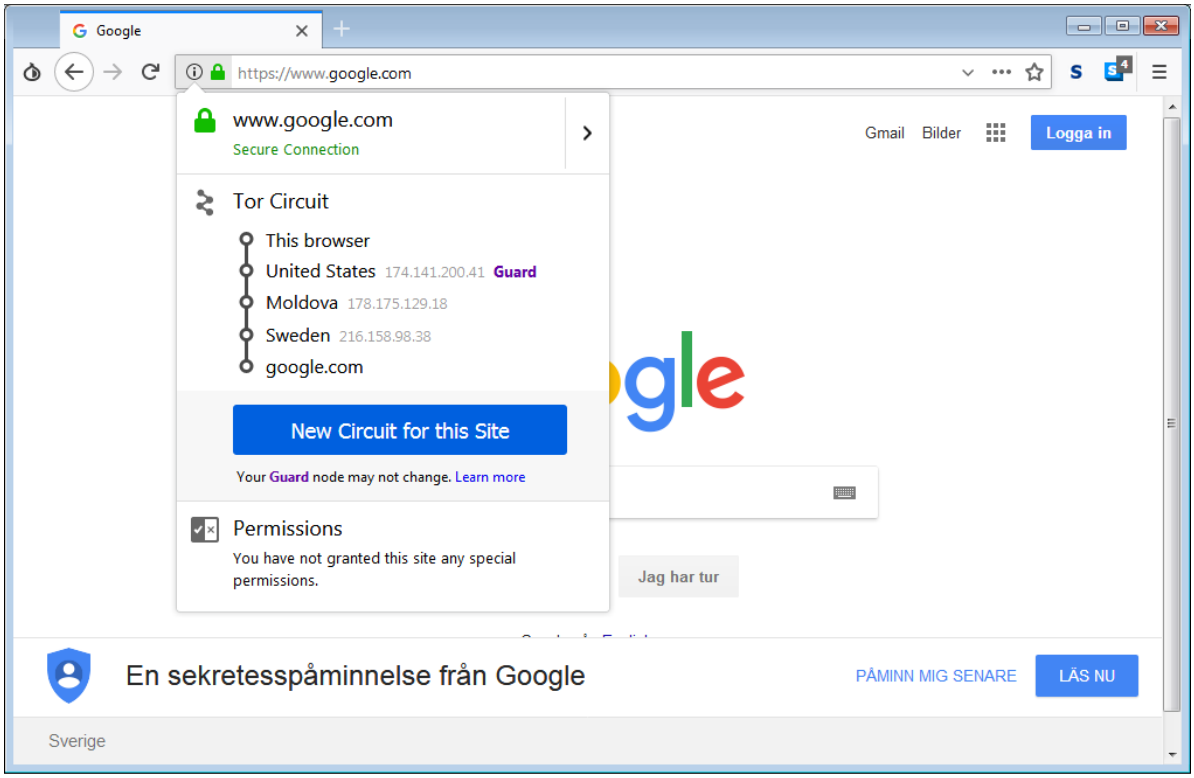

Figura 6 - Acessando o Google a partir da Suécia, via Tor Browser: detalhe do circuito Tor estabelecido

5. Exemplo prático na Web: denúncia anônima

Para desmistificar a premissa de que “privacidade só serve para ações ilegais”, podemos fazer um exemplo prático de uso do Tor como ferramenta de privacidade para um uso perfeitamente legítimo. Suponha que você precisa fazer uma denúncia anônima, por exemplo, por ter testemunhado um crime ou estar sendo vítima de assédio moral no trabalho. Algumas entidades (públicas ou privadas) permitem que isso seja feito por meio de um site, enquanto outras disponibilizam um endereço de e-mail para esse fim. Em ambos os casos, entretanto, sua privacidade pode não ser preservada. Afinal, ao acessar o site de denúncias, o seu endereço IP pode ser registrado e rastreado de volta a você (imagine se o alvo de uma denúncia de assédio moral for o chefe de Tecnologia da Informação da empresa!). Além disso, muitas ferramentas de e-mail deixam rastros na rede, incluindo o endereço de IP da máquina que enviou o e-mail em si como parte do cabeçalho da mensagem, um método comumente usado para evitar SPAM; também não é incomum que serviços gratuitos (como o Gmail ou Hotmail) exijam um número de telefone no momento do cadastro, o que dificulta registrar um endereço “anônimo” de fato. Neste cenário, uma tática interessante para permitir denúncias verdadeiramente anônimas é por meio do uso do Tor. Neste experimento, vamos assumir que o canal de denúncia é um e-mail, já que esconder seu IP ao visitar um site já foi mostrada nos experimentos anteriores.

Para, começar, use o Tor para visitar o GerrillaMail, no endereço https://www.guerrillamail.com/pt/. Este site fornece um serviço de e-mail descartável, sem exigir qualquer identificação do usuário. A interface do site deve ser similar à mostrada na Figura 7.

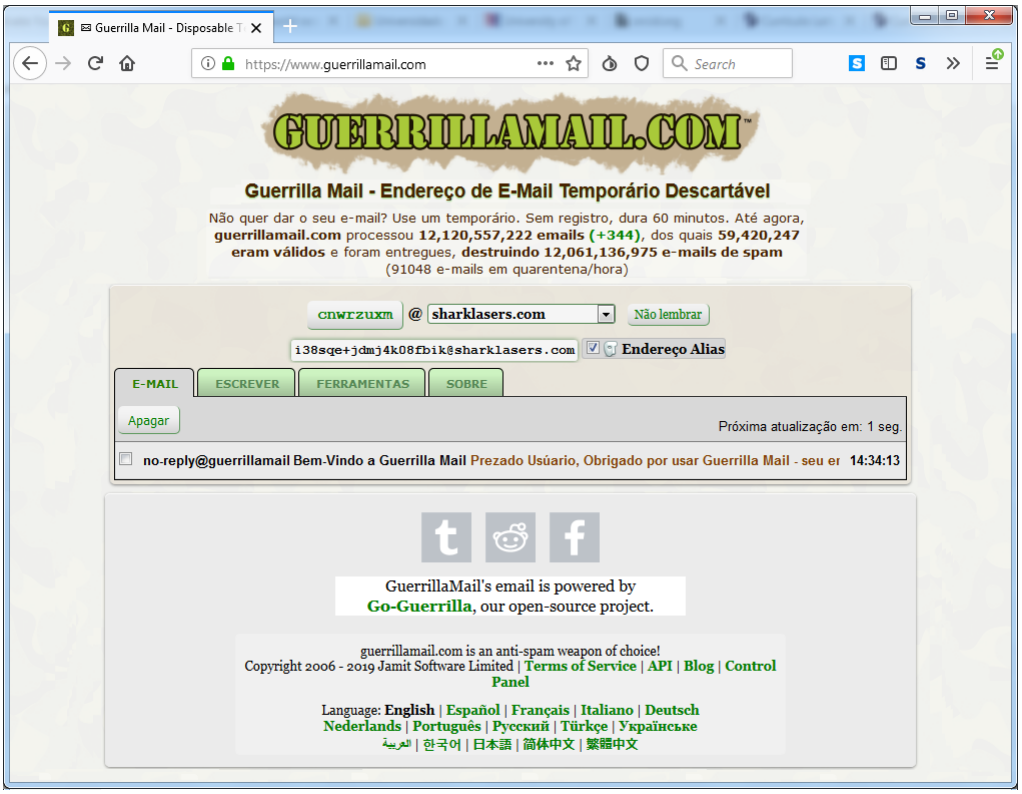

Figura 7 – Página inicial do GuerrillaMail, acessado via Tor

Basicamente, essa página gera um endereço de e-mail com aparência aleatória, como cnwrzuxm@sharklasers.com mostrado na Figura 7. O endereço que efetivamente aparece no e-mail, entretanto, é o "Endereço Alias", que consiste em uma versão embaralhada do endereço de fato, como é o caso do i38sqe+jdmj4k08fbik@sharklasers.com também mostrado na Figura 7. Essa medida de segurança é adotada porque o GuerrillaMail não exige qualquer senha, de modo que qualquer pessoa pode acessar a caixa de entrada de um endereço aleatório (para isso, basta clicar sobre o nome do endereço e trocar o seu valor). Porém, como não estamos interessados em receber resposta após a denúncia, esse detalhe não vai fazer muita diferença neste experimento.

Agora clique na aba "Escrever", para efetivamente criar a denúncia, o que deve abrir uma página similar à mostrada na Figura 8. Perceba que na parte de baixo da página há a seguinte mensagem: "*Attention: As countermeasure against spam, the following header will be added to outgoing email: X-Originating-IP:[91.219.237.244]*" – "Atenção: Como contramedida para evitar spam, o cabeçalho a seguir será adicionado ao e-mail enviado: X-Originating-IP:[91.219.237.244]". Ou seja, o endereço IP sendo observado pelo servidor do GuerrillaMail é informado ao destinatário. Se não fosse usado o Tor para acesso, isso revelaria uma informação que permitiria a identificação do emissor.

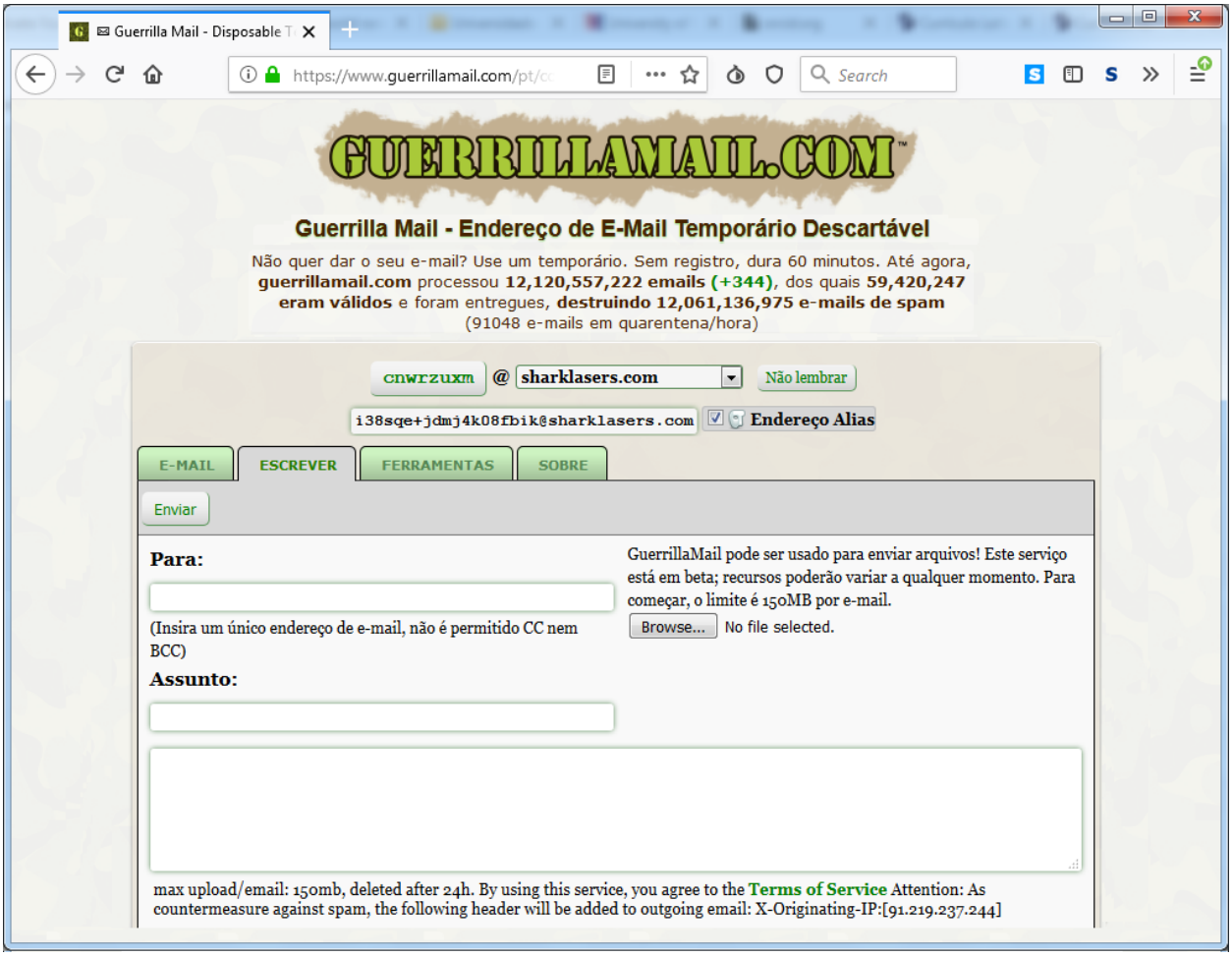

Figura 8 - Interface de escrita de e-mail no GuerrillaMail, acessado via Tor

Envie um e-mail para si mesmo, e perceba que não há nele qualquer informação sobre seu endereço IP: sugere-se ver o conteúdo completo da mensagem, incluindo cabeçalhos. Por exemplo, no Gmail, isso pode ser feito abrindo a mensagem, clicando nos 3 pontos verticais no alto à direita da tela, e selecionando a opção “Mostrar Original” (ou “Show Original”, na interface em inglês).

6. Visitando serviços escondidos, uma parte da Deep Web

Finalmente, vamos visitar um famoso site que usa o mecanismo de serviços escondidos do Tor: o Wikileaks, usado para denúncias internacionais sobre crimes de corrupção, espionagem, ambientais, etc. Para isso, acesse o seguinte endereço *.onion:*

http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page

A página que aparece deve ser semelhante à mostrada na Figura 9.

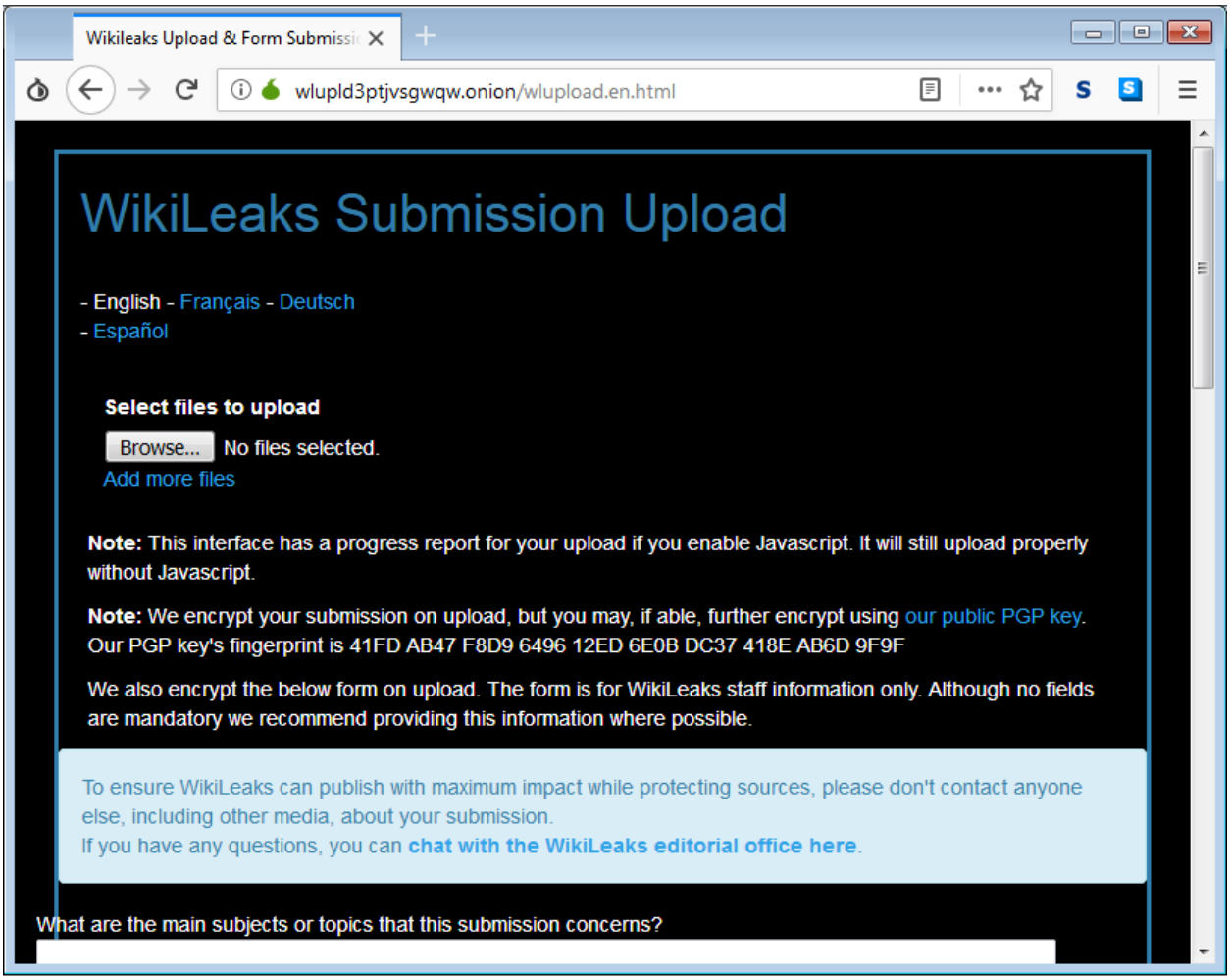

Figura 9 – Página do Wikileaks na Deep Web

E como achar outras páginas .onion? Afinal, não existe um mecanismo de busca como é comum na web tradicional, pois essa é exatamente a razão pela qual domínios *.onion* fazem parte da Deep Web: o fato de não haver *crawlers* que indexam todas essas páginas.

Para conseguir esse tipo de informação, basta visitar as chamadas “hidden wiki”, ou “wiki escondidas”. Esses sites são do tipo Wiki (qualquer pessoa pode editar) e contêm uma listagem de domínios *.onion* com sua respectiva descrição. Diversas dessas wikis podem ser encontradas na web simplesmente procurando por “hidden wiki” em um buscador como o Google. Também é possível acessar hidden wikis hospedadas na própria Deep Web. Embora seu endereço às vezes mude, no momento da escrita deste documento uma das principais hidden wikis podia ser encontrada em:

http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page

Acessar esse link por meio do Tor Browser deve te levar a uma página semelhante à mostrada na Figura 10. Ao navegar por essa página, é **MUITO IMPORTANTE** que você leia a descrição do site antes de visitá-lo: diversos dos sites listados contêm conteúdo ilegal e/ou imagens que pessoas normais podem considerar perturbadoras. Seções como “Email / Messaging” (envio de mensagens de forma privada), “Whistleblowing” (para denúncias anônimas) e “Books” (livros, alguns deles raros e de domínio público, outros com direitos autorais) costumam ser razoavelmente seguras para navegação. Outras seções exigem um pouco mais de cautela, como qualquer navegação na web tradicional.

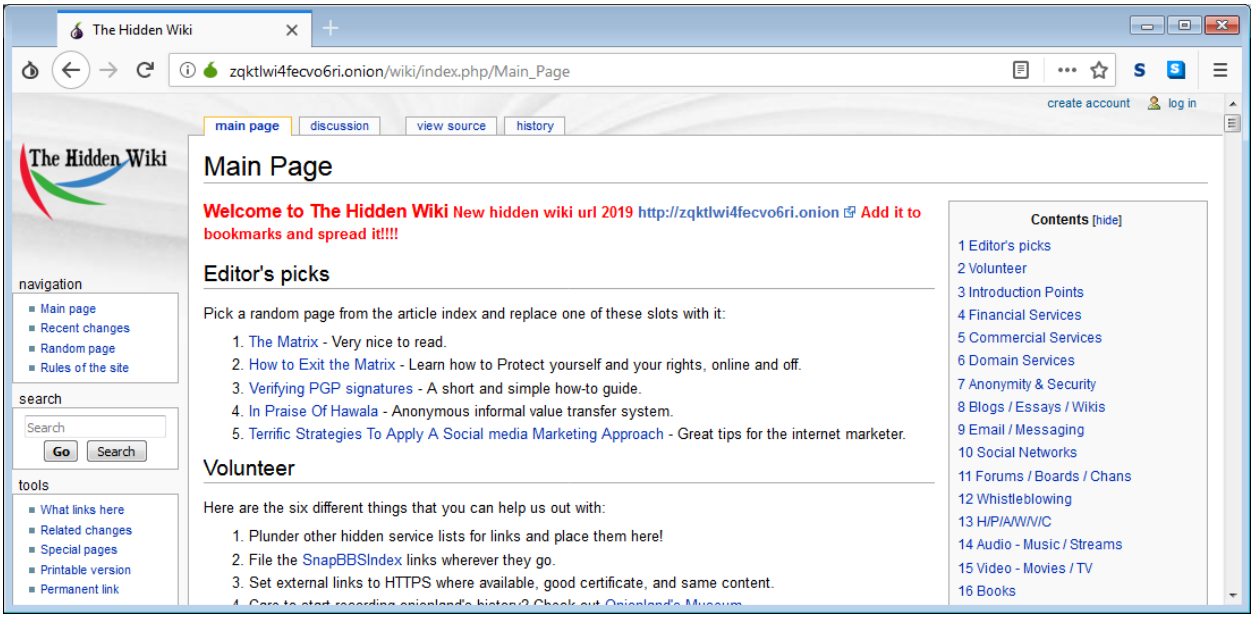

Figura 10 – Hidden wiki na Deep web

Finalmente, perceba que se você tentar acessar a Hidden Wiki mostrada na Figura 10 (ou qualquer outra página *.onion*) usando um navegador comum, sem Tor, você irá receber uma mensagem de erro. Afinal,

esses sites só são acessíveis por usuários que estejam executando o protocolo de serviços ocultos do Tor. Esse efeito de “esconder IP de servidores” do Tor é ilustrado na Figura 11, que mostra a conexão entre:

- O circuito Tor estabelecido pelo usuário, passando pelos EUA, Áustria e França
- O circuito Tor do site visitado, composto por três computadores. A localização desses computadores não é mostrada, de modo que eles são identificados apenas como “Relay”, porque o Tor Browser do usuário não consegue saber os endereços IP desses nós (da mesma forma que o site visitado não é informado sobre os endereços IP que compõem o circuito Tor do usuário).

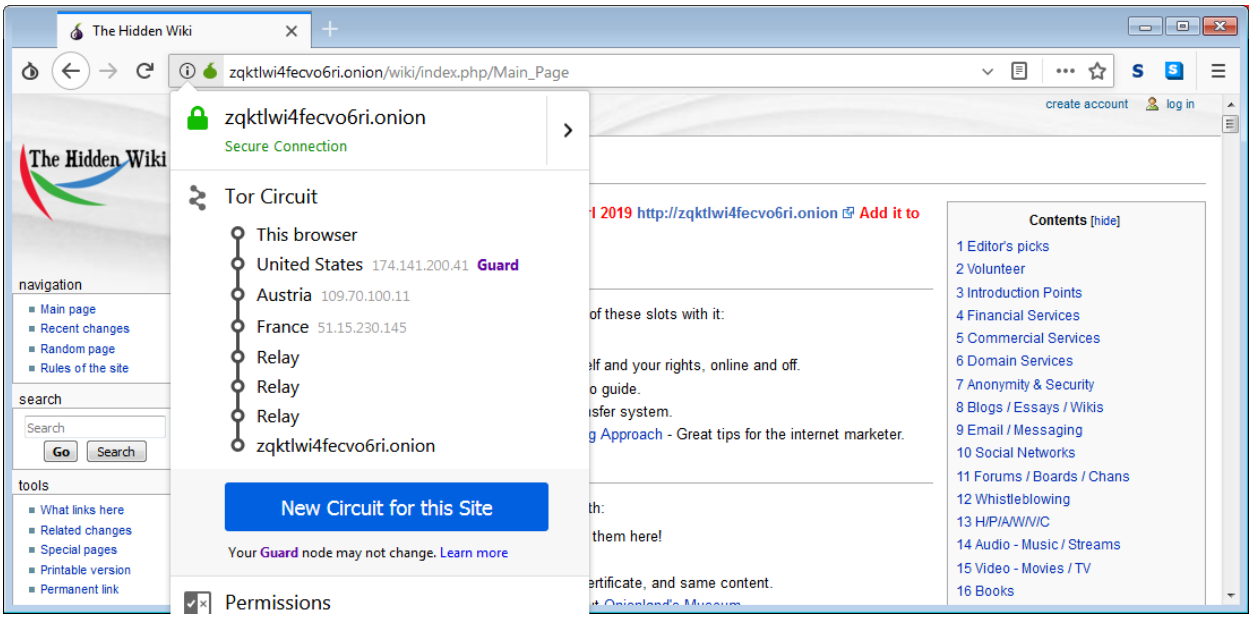

Figura 11 - Hidden wiki na Deep web: o circuito Tor estabelecido conecta dois circuitos, um do usuário e outro do site sendo visitado.

7. Considerações finais

Isso conclui o experimento. Lembre-se: como qualquer ferramenta, o Tor pode ser usado para fins lícitos ou não. Portanto, cautela no seu uso para não infringir preceitos legais e morais é essencial: “Conhecimento é poder” [Francis Bacon?], mas “Com grande poder, vem grande responsabilidade” (Tio Ben).