TÉCNICAS DE USO PRIVATIVO DA INTERNET

Weder Eduardo Pedro

Bacharel em Sistemas de Informação

Dorival Moreira Machado Junior[1]

Mestre em Tecnologias da Inteligência e Design Digital

RESUMO

Independentemente das intenções, algumas pessoas possuem um grande poder nas mãos. Trata-se da habilidade, ou, simplesmente,do fato de ter ao seu alcance recursos tecnológicos que permitem o acesso às informações sigilosas, seja para vigilância e investigação de ameaças terroristas, interceptação de mensagens particulares, ou até mesmo, monitoramento dos dados de navegação, de usuários, de todo o mundo. Com o caso delatado, por Edward Snowden, e outros casos espalhados pela mídia, torna-se viável adotar técnicas que possam diminuir a vulnerabilidade do usuário. Este artigo, tem como objetivo apresentar formas mais seguras de se utilizar a Internet, observando com maior critério a privacidade de identidade. Tal pesquisa, então embasada nos relatos de Edward Snowden, refere-se às formas mais comuns de uso na Internet e que são: a navegação, a troca de e-mails e a utilização de *chats*. São demonstradas formas que dificultam o rastreamento e a aquisição de informações, podendo tais recursos serem aplicáveis, desde a usuários domésticos, até aqueles com conhecimentos mais avançados, que buscam maior privacidade.

Palavras-chave: Internet. Snowden. privacidade. rastreamento. informações.

[1] dorivaljunior@libertas.edu.br

1 INTRODUÇÃO

Tem sido destaque na mídia, vários casos de invasão de privacidade e quebra de sigilo(CAMPI, 2015) (MACEDO, 2015), seja em e-mails, contas bancárias ou até mesmo nas redes sociais. A repercussão desses acontecimentos deixa o questionamento se existe uma forma mais segura de se navegar na Internet, resguardando a identidade do usuário. Edward Snowden ex-agente da NSA (*National Security Agency*) revela a Glenn Greenwald, uma série de documentos que conseguiu enquanto prestava serviços a NSA, que mostram dados de monitoramento de usuários, do mundo inteiro, e algumas ferramentas que aumentam a segurança mediante tal rastreamento (GRENNWALD, 2014).

Não compete, a este trabalho, realizar testes exaustivos buscando encontrar falhas ou erros nas ferramentas, mas sim, poder apresentar a forma de uso e o funcionamento das mesmas, bem como de que forma elas podem ajudar. Também não é objetivo fazer um comparativo, nem eleição de ferramentas, mas realizar uma proposta de uso, com base nas ferramentas mencionadas pelo ex-agente da NSA (GRENNWALD, 2014, p. 25).

O estudo em questão visa colaborar com usuários domésticos, etambém com aqueles que tenham conhecimento avançado, pois, a maioria das pessoas que usam Internet, sequer sabem, que existem ferramentas que ajudam a diminuir os riscos de invasão, ou até mesmo de rastreamentos de suas atividades, ou seja, reforço na garantia da privacidade. Por motivos como esses, faz-se necessário um estudo sobre o assunto, uma vez que é real o aumento de usuários, da quantidade de dados colocados na rede (IX.BR, 2015), e do interesse das pessoas, principalmente do meio político e econômico, querendo ter acesso a essas informações.

Para isto, foi realizada uma pesquisa exploratória, com base nos relatos de Edward Snowden, recentemente publicado (GRENNWALD, 2014), no qual são relatadas informações confidenciais de que, o Governo Americano estaria rastreando comunicações eletrônicas dos americanos, e até mesmo de governantes de outros países. Estudando técnicas e ferramentas citadas pelo Snowden, espera-se alcançar, como resultado, uma forma mais privativa de utilizar a Internet.

Após as revelações pode-se observar uma grande movimentação em vários países, entre eles o Brasil (DIAS, 2013), visando a melhoria nas condições dos usuários da Internet, buscando alcançar a liberdade na “Grande Rede”.

2 REVISÃO BIBLIOGRÁFICA

Quem tem a facilidade de interceptar mensagens e levantar informações sigilosas, tem um grande poder em suas mãos. Com o aumento de ameaças e riscos de ataques terroristas, intensificaram-se as investigações, a vigilância e o rastreamento de possíveis conversas de terroristas ou, com este fim. Ainda com outra visão, pessoas mal-intencionadas usam desse poder para obstruir conversas, interceptar mensagens particulares e até mesmo criar uma ampla rede de monitoramento e análise dos dados de navegação, de usuários, de vários lugares do mundo, como a rede criada pela NSA (*National Security Agency*) delatada por Edward Snowden, através de seus contatos com Glenn Greenwald e outros jornalistas.

GREENWALD, (2014, p. 97) afirma que os documentos levantados por Edward Snowden "era espantoso" pelo tamanho e pela abrangência. Vários programas de vigilância apresentados por Snowden tinham como alvo, países como França, Brasil, Índia e Alemanha. Uma vigilância, em massa, indiscriminada. O acervo revela recursos técnicos usados para interceptar comunicações, o monitoramento pela NSA de servidores de Internet, satélites, redes de fibra ótica e telefonia. Uma enorme teia de vigilância de cidadãos, tanto americanos quanto não americanos.

Todo acervo fornecido por Edward Snowden revela um grande plano de espionagem e monitoramento, tanto de cidadãos norte-americanos, quanto de outros países, entre eles o Brasil, tendo como principais alvos a Presidente Dilma Rousseff, o Ministério Minas de Energias e a Estatal Petrobrás (G1, 2015).

Uma reportagem do Jornal de The Guardian (BALL, 2014) relata dados fornecidos por Snowden sobre um programa de rastreamento chamado PRISM, o qual tem acesso a dados das maiores empresas de Internet no mundo, entre elas, Facebook, Yahoo!, Apple, Google e o Outlook. As empresas citadas alegaram não participar deste projeto, e, não proporcionar acesso ilimitado a seus servidores. Elas relatam que só fornecem dados à NSA, quando possuem um mandato para isso (ARRUDA, 2015).

Os documentos que Snowden apresentou, denunciando a espionagem de usuários do mundo inteiro através do PRISM, entre eles referências à Presidente Dilma Rousseff, cooperaram com o entendimento do governo brasileiro, de que, se tornava urgente a necessidade da discussão e aprovação dos temas abordados naLei 12.965/14 (CASA CIVIL, 2015). Os relatos também levaram o governo a tomar medidas contra empresas como a

Google e o Facebook, obrigando a hospedarem os dados dos usuários em território nacional em vários servidores espalhado pelo Brasil (DIAS, 2013).

De acordo com CULTURA DIGITAL (2014), *a* Lei 12.965/14 conhecida como Marco da Internet, foi sancionada pela Presidente Dilma Rousseff no dia 23/04/2014 e visa a proteção à privacidade do usuário, à liberdade de expressão e à garantia da neutralidade da rede. Tal texto é descrito da seguinte forma:

> A proteção aos dados dos internautas é garantida e só pode ser quebrada mediante ordem judicial. Isso quer dizer também que se você encerrar sua conta em uma rede social ou serviço na Internet pode solicitar que seus dados pessoais sejam excluídos de forma definitiva. Afinal, o Marco Civil da Internet estabelece que os dados são seus, não de terceiros. Por isso, fique atento com relação à atualização dos termos de uso dos serviços e aplicativos que você utiliza! Outra inovação promovida pelo Marco Civil da Internet é a garantia da privacidade das comunicações. Até a Lei entrar em vigor o sigilo de comunicações não era válido para *e-mails*, por exemplo. A partir de agora o conteúdo das comunicações privadas em meios eletrônicos tem a mesma proteção de privacidade que já estava garantida nos meios de comunicação tradicionais, como cartas, conversas telefônicas, etc (CULTURADIGITAL,2014).

Medidas com o intuito de impedir esse amplo rastreamento, estão sendo tomadas em vários países, segundo G1(2015). A partir do dia 01/06/2015 foi suspenso temporariamente o programa de coleta de dados e registros telefônicos da NSA revelado por Edward Snowden em 2013. Um projeto de lei chamado Freedom Act (Lei da Liberdade) dará acesso às informações somente após estudosdos casos apresentados pela NSA. Caso haja a aprovação da lei no senado, será mais um avanço conquistado através das revelações de Edward Snowden.

Um outro fato que fortalece o embasamento deste trabalho nos relatos do Snowden é a obtenção do prêmio “Nobel Alternativo” dos Direitos Humanos, como reconhecimento à melhoria na condição de vida da humanidade. Em 2015 o documentário CitizenFour que descreve o escândalo revelado por Edward Snowden ganhou o Oscar de melhor documentário OGLOBO (2015).

3 MATERIAIS E MÉTODOS

Para o desenvolvimento da pesquisa, foi realizado um experimento em laboratório, replicandocada uma das situações básicas mais comumente realizadas pelos usuários e que são: navegação, *chat* e envio de e-mail. Em um primeiro momento foi realizado o acesso na forma tradicional, em seguida, os mesmos acessos, porém utilizando-se de recursos que

fortalecem a segurança dos dados, além de dificultar o seu rastreamento. É importante salientar que não se pode garantir 100% de eficiência dos recursos então testados, porém com base nos testes realizados, é visível que existe um processo de criptografia envolvido bem como uma melhoria na questão da privacidade.

3.1 Descrição do laboratório de experimento

Para realização do experimento foi utilizado uma máquina com um processadorIntel (R) core (™) I7-2640M CPU @ 2.80GHz, com 6GB de Memória RAM, com HD de 500GB e o sistema operacional Windows 7 Professional Service Pack 1 de 64 bits. Em outras palavras, uma máquina de porte comum e acessível.

3.2 Instalação e configuração básica dos recursos de segurança

Uma das principais ferramentas citadas por Snowden, e apontada como a mais utilizada para se manter longe da espionagem da NSA, foi o Linux Tails ou Tails SO (TAILS,2014). Este é um sistema operacional livre. O código fica disponível a qualquer um que queira participar, com melhorias e estudos, principalmente, no que se refere à segurança e privacidade.

Após os relatos de espionagem virem à tona, vários técnicos, estudiosos e até hackers, começaram a colaborar para o desenvolvimento dessa ferramenta, deixando cada vez mais invisível aos olhos dos que tentam espionar e obter informações acerca do que acontece na Internet (TAILS, 2014).

Conforme TAILS (2014), o Tails funciona de forma simples e pode ser gravado em um cd/dvd ou pendrive. Pode ser iniciado em qualquer máquina, com qualquer sistema operacional. Basta iniciar com um *Boot* no cd/dvd ou pendrive, onde é carregado e iniciado, usando somente a memória RAM da máquina.

Nenhum dado que é acessado, gravado ou transferido fica registrado na memória (FOROUZAN; MOSHARRAF, 2011), pois, não envolve o uso de HD. O registro acontece, somente se o usuário quiser, e mesmo assim, será necessário configurar senhas de acesso a discos rígidos.

O Tails Linux, tem um recurso de segurança para auxílio na sua utilização em ambientes tradicionais como um café, uma *lan house*, entre outros. É o recurso de

camuflagem. Sua aparência simula o Windows 8.1. Quem observa um usuário operando o Tails, não sabe que se trata de tal sistema. Este recurso parece ser algo irrelevante, porém evita a atenção de curiosos em relação a um sistema operacional menos comum utilizado na máquina.

Para conseguir uma forma de navegar mais segura e privativa, o Tails utiliza o navegador Tor, impossibilitando o rastreio de seu IP inicial, pois ele força o uso de vários nós intermediários no mundo inteiro, tornando sua navegação anônima.

O Tor também permite uma navegação sem censura alguma, permitindo você, também,possa navegar no submundo da Internet. Desta forma é necessário que o usuário saiba o que quer e o que vai acessar (TORPROJECT, 2014).

Utilizando o padrão de criptografia SSL (IBM, 2015), o Tor permite que os acessos sejam de maneira segura, criando um canal criptografado entre um servidor Web e um navegador para garantir que todos os dados transmitidos sejam seguros.

O Navegador Tor, trabalha como qualquer outro navegador. Inicia-se o aplicativo e aguarda a conexão com um servidor Tor aleatório. Após a conexão, é criada a teia de rastreio de IP. Compatível com outros sistemas operacionais, o Tor pode ser usado separadamente do Tails, ou seja, não é uma ferramenta exclusiva Linux.

Para trabalhar com *chat* o Tails disponibiliza o Pidgin, um mensageiro instantâneo que utiliza código aberto, que suporta vários protocolos de comunicação instantânea. Esta ferramenta, também, se mostra muito útil trabalhando de forma separada em outros sistemas operacionais com o Windows.

Quando se fala de segurança, o Pidgin vem configurado com a ferramenta de criptografia de *chat* OTR (OTR, 2015), criando um ponto-a-ponto, enviando mensagens criptografadas em um protocolo de alto nível de dificuldade de quebra (PIDGIN, 2015). O *chat* OTR foi citado por GREENWALD, (2014, p.26) como ferramenta essencial para comunicação com Edward Snowden sem que alguém interceptasse as mensagens.

O Pidgin, não diferente das outras ferramentas citadas, é simples e bem especifico. Na parte de configuração, dependendo do provedor de mensagens que utilizar, pode ser necessário liberar algumas permissões de acesso a outras máquinas e à aplicativos considerados com menor segurança. No caso do teste com o Google Talk, foi necessário ativar a opção de *login*, nas configurações de conta do Google.

Após os relatos do Snowden, membros da MIT (Instituto de Tecnologia de Massachusetts) em conjunto com desenvolvedores de Harvard e do CERN (Organização Europeia para Pesquisa Nuclear) iniciaram um projeto chamado ProtonMail.

O ProtonMail consiste em um serviço de e-mail, com sua base na Suíça, e que permite envio e recebimento de e-mails criptografados, tornando a comunicação mais segura possível. O fato da base se localizar na Suíça, ajuda na segurança, pois, na Suíça as leis de proteção das empresas e dos indivíduos são mais fortes, segundo MORAES, (2014).

3.2.1 Linux Tails

Para a instalação e configuração do Linux Tails, foi feito o download do site oficial do projeto (TAILS, 2014), onde seguiu-se os passos de instalação sugeridos no próprio site. O processo todo resume-se em gravar uma imagem em DVD ou Pendrive da ISO do Linux Tails. Em seguida reinicializar o computador, utilizando este novo sistema no boot. Comojáfoimencionado, o sistema executa em memória RAM, não fazendo qualquer tipo de registro permanente no computador.

Feito isto o Linux Tails iniciou com suas telas de configuração de linguagem, segurança e aparência, ao selecionar as opções desejadas o sistema inicializou-se com sucesso.

Esta ferramenta já disponibiliza o navegador Tor e o Pidgin instalados e configurados.

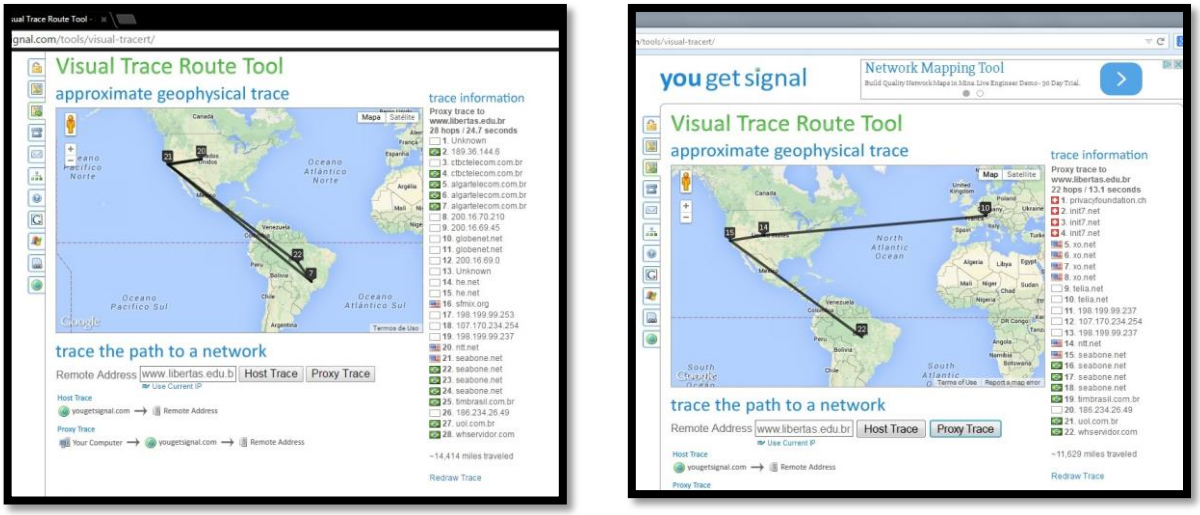
3.2.2 Navegador Tor

Como o Tor já vem configurado no Tails, os testes foram realizados no Windows. Para a configuração no Windows, o Navegador Tor foi baixado no site oficial do projeto (TORPROJECT, 2014). Após instalado, utilizando as configurações padrões (tradicional *nex-next-install*), o aplicativo iniciou, funcionando normalmente, bastando executar o navegador e estabelecer a ligação. O intuito geral do Tor, basicamente, é prover um caminho mais extenso da conexão, forçando os pacotes a passarem por diversos roteadores antes de serem liberados para a Internet. A FIGURA 1-a apresenta um *traceroute* (rastreamento de rota), que neste caso foi feito através do YOU GET SIGNAL, (2015). Este demonstra os saltos que um pacote faz até chegar ao endereço www.libertas.edu.br (escolhido aleatoriamente apenas para teste da

pesquisa), enquanto que na FIGURA 1-b, é demonstrando o acesso ao mesmo destino, porém utilizando-se do Tor.

Na FIGURA 1-a, observa-se que o *traceroute* detecta como ponto de origem o Brasil (o que realmente é), passa por diversos nós, em específico o ntt.net (nó 20), local de hospedagem do *traceroute* utilizado na pesquisa. Por fim, o caminho aponta ao Brasil, local de destino onde o site www.libertas.edu.br está hospedado.

Na FIGURA 1-b, observa-se que o traceroute detecta como ponto de origem a Suíça (o que não acontece na realidade, mas é o ponto que o Tor permitiu no momento do teste para iniciar as conexões). A conexão passa por diversos nós, em especifico o ntt.net (neste teste referenciado como nó 14), e por fim chega ao Brasil.



(a) (b)

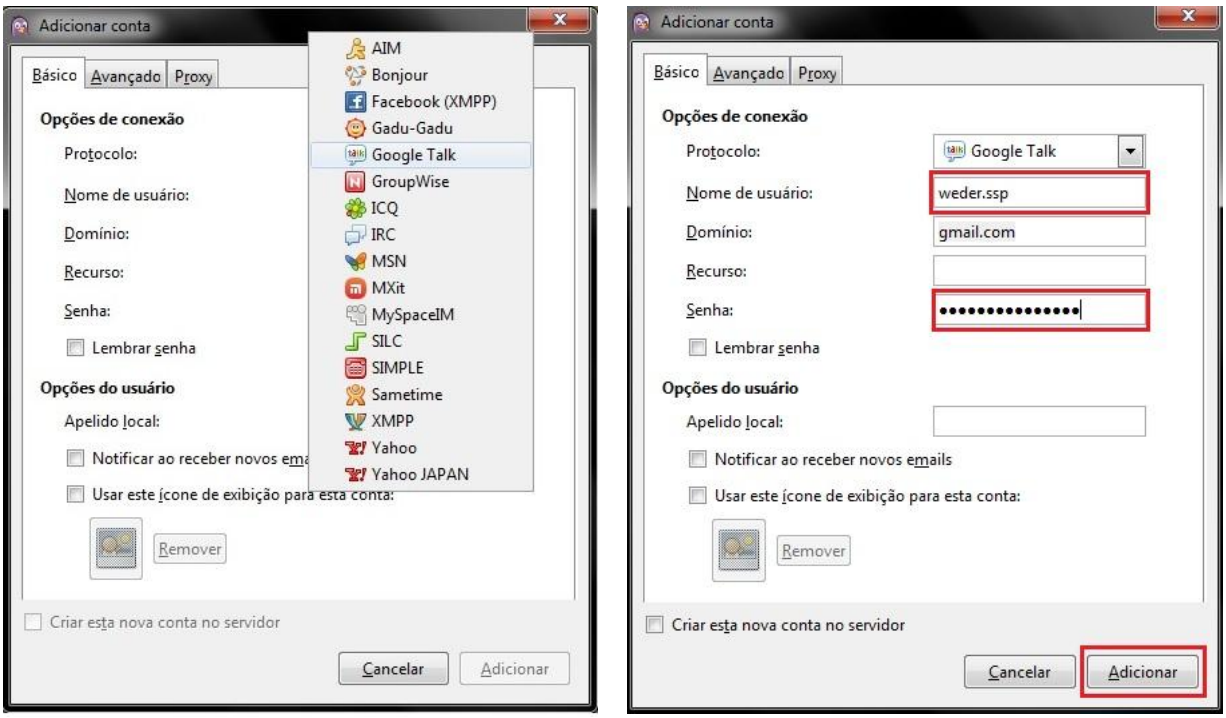
FIGURA 1 - *Print* da rota de acesso ao siteww.libertas.edu.br
Fonte: Próprio autor

3.2.3 Pidgin Mensageiro Instantâneo

Para a configuração no Windows, o Pidgin foi baixado pelo site oficial do aplicativo (PIDGIN, 2015), executado o *setup* e instalado. Após a instalação foi necessário baixar e instalar o *plug-in* do chat OTR pelo site oficial do desenvolvedor (OTR, 2015).

Após a instalação foi iniciado o Pidgin e configurado conforme apresentado na FIGURA 2.

A FIGURA 2-a mostra a tela de configuração do Pidgin, onde está sendo escolhido o provedor do *chat*, que no teste em questão é o Google Talk. A FIGURA 2-b mostra a inserção do usuário e senha, ao clicar no botão adicionar a configuração da conta já estará realizada.



(a) (b)

FIGURA 2 - *Print* da tela de configuração
Fonte: Próprio autor

A FIGURA 3 mostra a tela do Pidgin já conectado, informando a conta conectada, a quantidade de amigos conectados, assim como total de amigos.

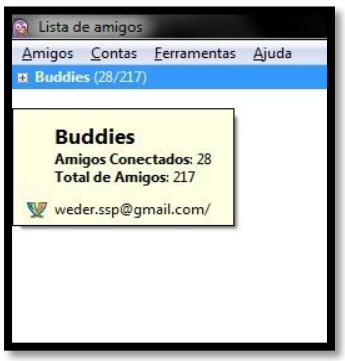


FIGURA 3 - *Print* da tela inicial do Pidgin conectado.
Fonte: Próprio autor

3.2.4 ProtonMail

O ProtonMail é acessado pelo site oficial (PROTONMAIL, 2015), onde são inseridos usuário e senha. O acesso ao ProtonMail é realizado de forma simples como em qualquer outro gerenciador de e-mail, basta inserir o usuário e a senha que já se conecta.

Na FIGURA 4 pode-se observar o *login* no ProtonMail sendo realizado.

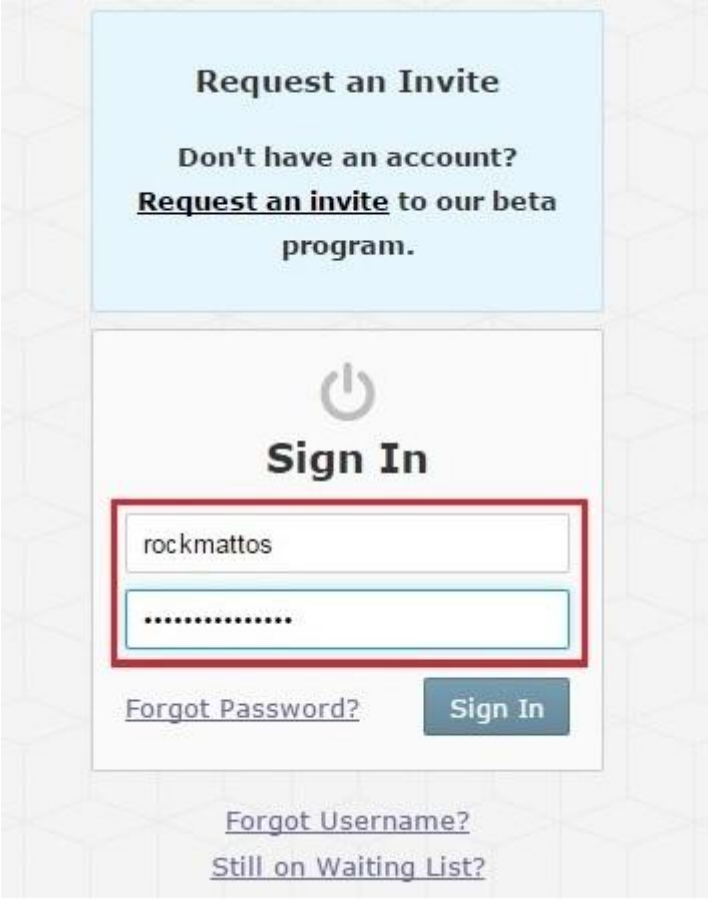


FIGURA 4 - *Print* da tela de login do ProtonMail
Fonte: Próprio autor

3.3 Realização dos testes

Os testes foram realizados no ambiente informado, e coletadas imagens como registro dos testes realizados. Todas as ferramentas citadas foram testes de mesa em suas maneiras básicas de uso, de modo que possam ser tiradas conclusões com base nos resultados obtidos.

4 RESULTADOS

A seguir, são demonstradas as formas de uso tradicional e na sequência, estes mesmos usos, porém utilizando-se de recursos de reforço na segurança e privacidade.

4.1 Uso do Tails

De acordo com os testes realizados, o Tails apresenta uma forma fácil de uso. Possibilita logo no início a escolha do idioma desejado e a forma de conexão com a Internet, além de te dar a opção de camuflar o sistema. Ele também disponibiliza um manual com os meios de uso do sistema operacional, sempre aconselhando a utilizar o Tails e suas ferramentas da maneira mais segura, mostrando que usando apenas a memória RAM, nada do que foi acessado pode ser analisado depois de desligar a máquina.

4.2 Navegação na forma tradicional

Na FIGURA 5 pode-se observar que em um ambiente de navegação normal (no caso apresentado, usando o navegador Chrome da Google) o Wireshark localiza o IP do site acessado: www.libertas.edu.br, IP: 187.17.98.154. O Wireshark conseguiu também localizar os pedidos de confirmação do DNS.

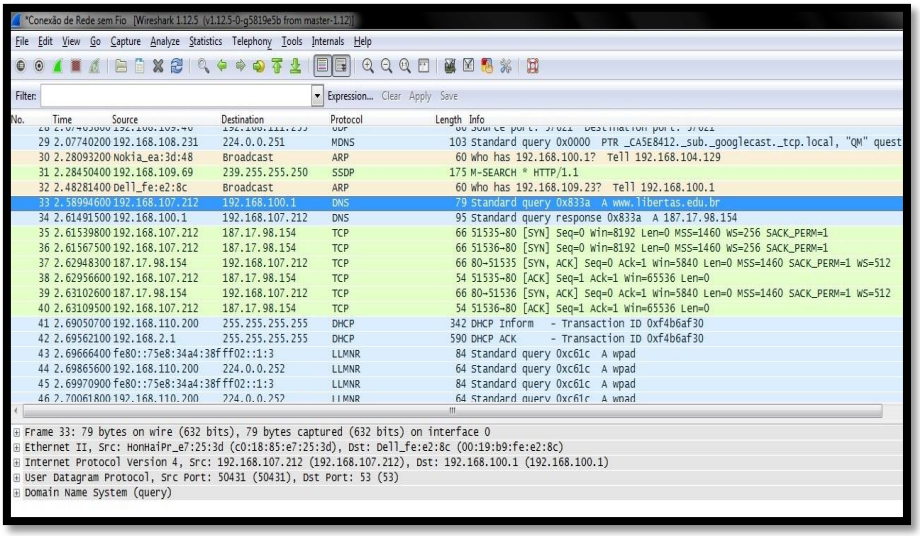


FIGURA 5 - *Print* da Busca do IP do Site da Libertas no Wireshark
Fonte: Próprio autor

A FIGURA 6 apresenta o pacote localizado pelo Wireshark informando os dados do site de destino (www.libertas.edu.br).

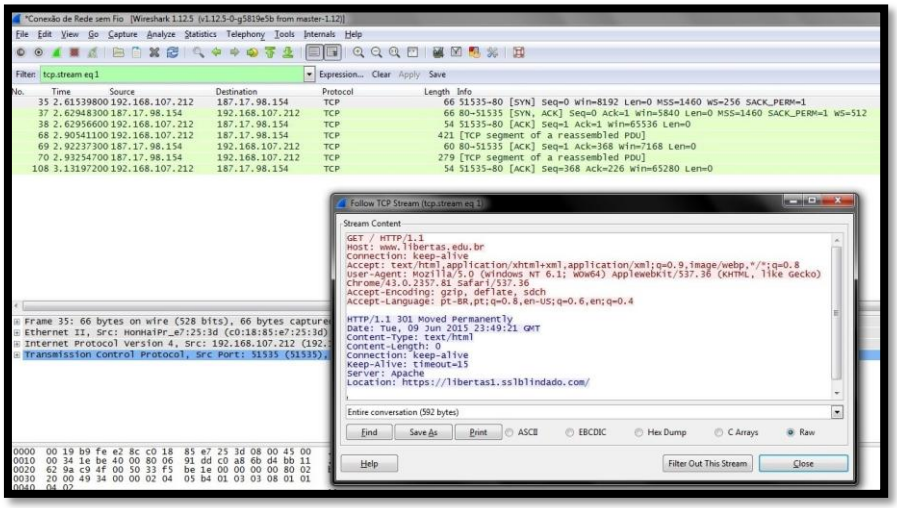


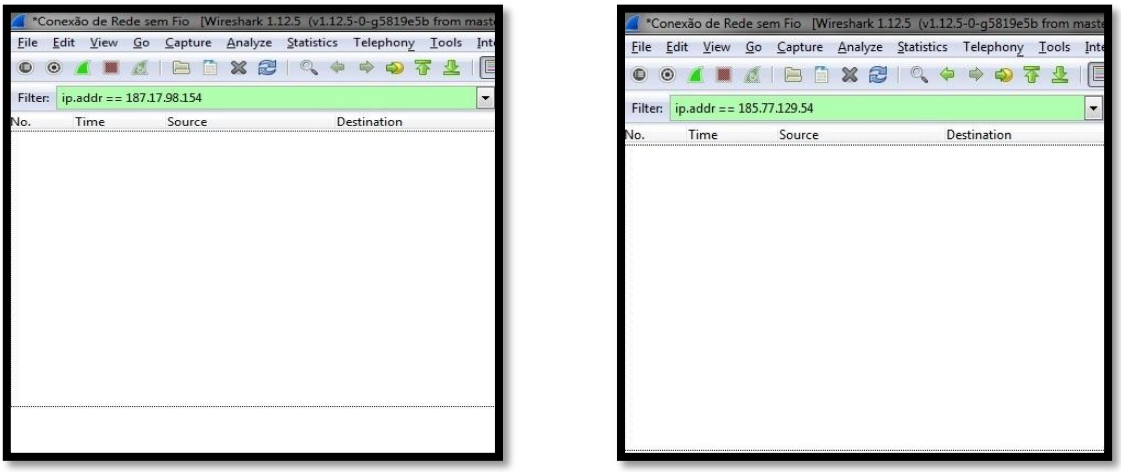
FIGURA 6 - *Print* da tela do Wireshark mostrando o pacote com os dados do site acessado
Fonte: Próprio autor

4.3 Navegação utilizando recurso de reforço na segurança

A FIGURA 7 mostra os nós do Tor até chegar no ponto de partida fictício (o ponto o qual a rede Tor quer que a Internet acredite ser a origem). Nela pode-se observar que ele passa por 3 camadas principais até chegar no site de destino.

FIGURA 7 - *Print* da tela do Tor acessando o site da Libertas e mostrando as camadas
Fonte: Próprio autor

A FIGURA 8-a mostra a busca pelo IP do site acessado, desta vez com reforço de segurança, usando o Navegador Tor. Como pode-se observar na imagem, após efetuada a busca por pacotes com o IP 187.17.98.154, não retornou nenhum dado. Já a FIGURA 8-b mostra a busca pelo último IP de saída do Tor e que não foi possível localizar também.



(a) (b)

FIGURA 8 - *Print* da tela do Wireshark buscando o IP do site da Libertas e do IP de saída do Tor
Fonte: Próprio autor

A FIGURA 9 mostra a busca pelo primeiro IP de saída do Tor e seu pacote completamente criptografado, impossibilitando a descoberta do destino e conteúdo do pacote.

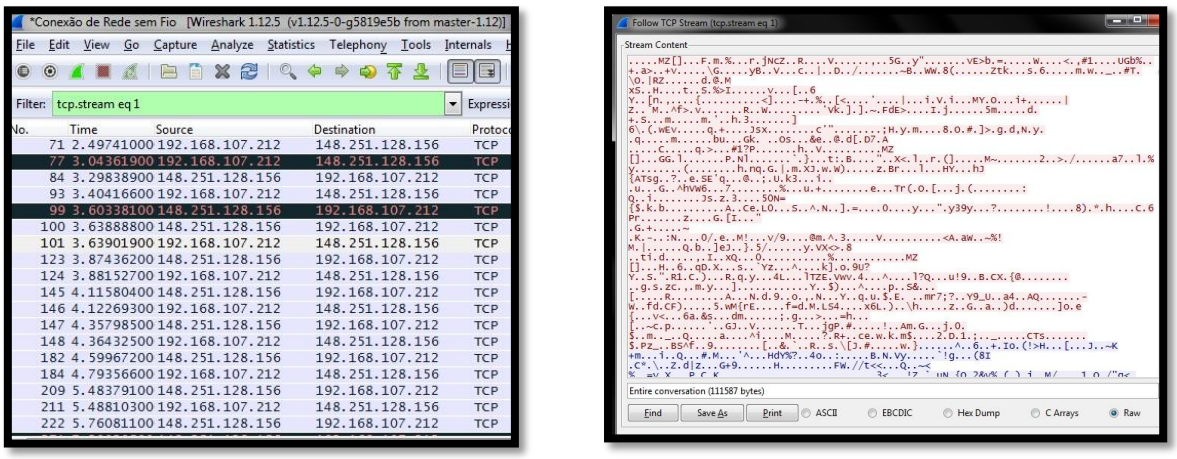


FIGURA 9 - *Print* da tela do Wireshark buscando o pacote criptografado do primeiro Ip do Tor
Fonte: Próprio autor

4.4 Chat Pidgin

Com o chat Pidgin, mesmo não ativando o OTR foi possível observar o reforço na segurança. A FIGURA 10 apresenta um pacote do Pidgin usando o Google Talk capturado pelo Wireshark com seus dados criptografados.

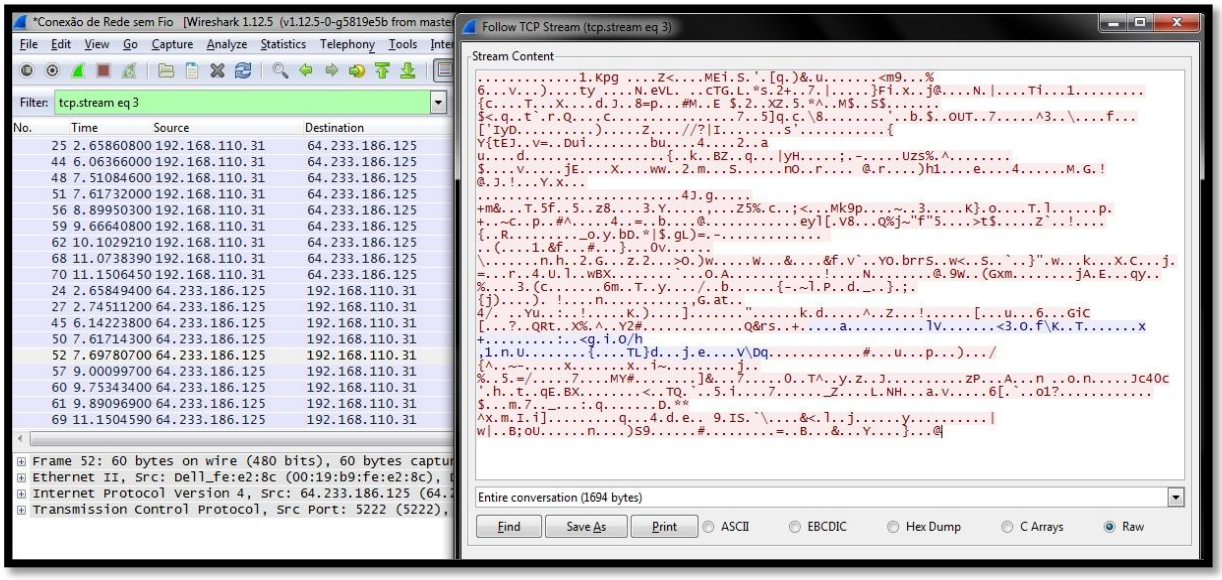


FIGURA 10 - *Print* do pacote criptografado do Pidgin capturado pelo Wireshark
Fonte: Próprio autor

4.5 Envio de e-mail pelo ProtonMail

Os testes com o ProtonMail foram realizados de forma mais simples, pois ele mesmo faz todo o processo que aumenta e define a segurança e a privacidade do usuário.

O ProtonMail oferece a possibilidade de inserir chaves de segurança para que, somente quem tiver a chave consiga abrir o e-mail e ler a mensagem escrita conforme apresentado na FIGURA 11. Possibilita, também, que o destinatário possa responder o e-mail pelo ProtonMail, mantendo a segurança da comunicação. O Proton oferece no momento da leitura uma ferramenta de gerenciamento de e-mail, que possibilita responde-lo pelos mesmos meios.

Sendo assim, a comunicação usando o ProtonMail pode ser feita com segurança tanto entre usuários ProtonMail, quanto um correspondente que não use o ProtonMail, esta comunicação ficaria como apresentado na FIGURA 12.

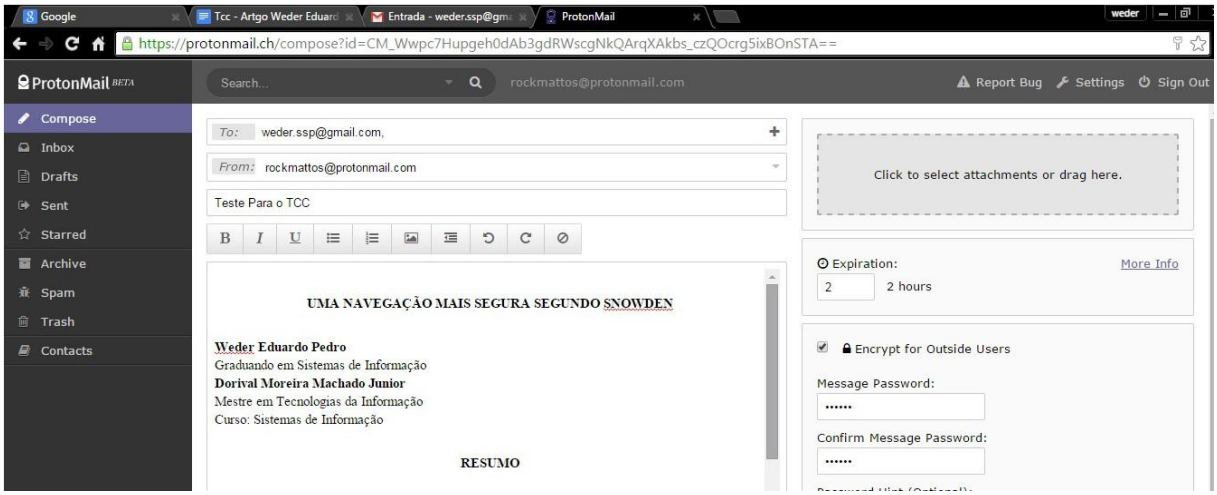


FIGURA 11–Enviando e-mail pelo ProtonMail inserindo chave de segurança
Fonte: Próprio autor

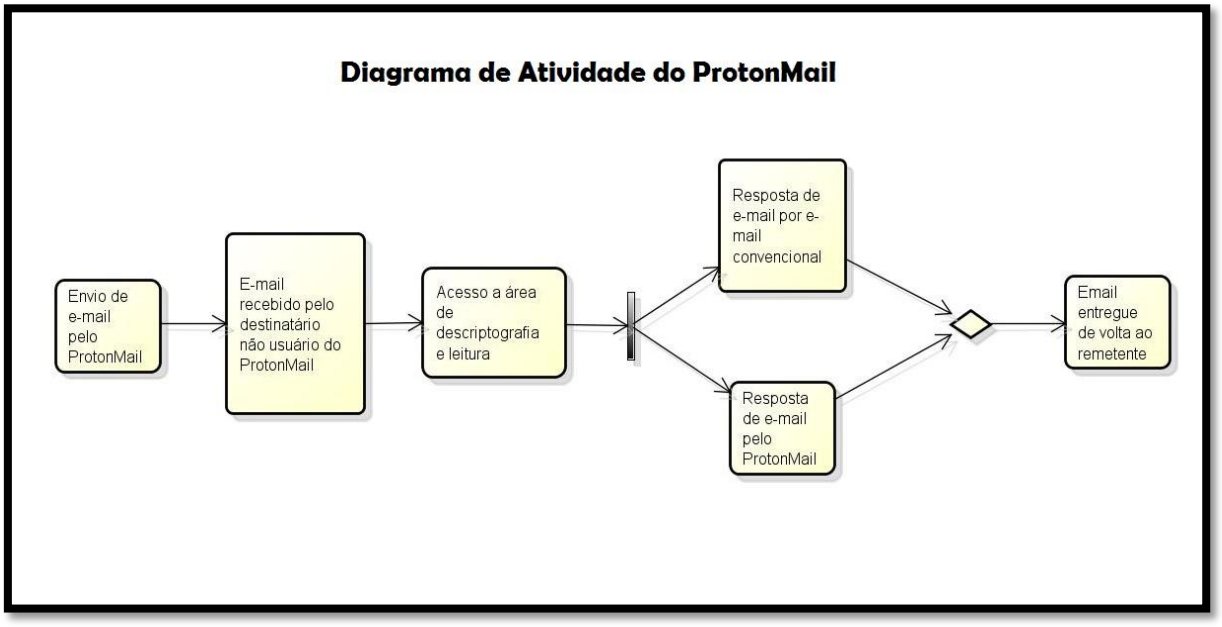


FIGURA 12 - Diagrama de Atividade da comunicação com um correspondente tradicional
Fonte: Próprio autor

5 CONSIDERAÇÕES FINAIS

O Linux Tails usando a memória RAM da máquina, deixa a certeza de que os dados acessados são eliminados assim que se desliga o equipamento, impossibilitando a verificação do que foi acessado.

Nos testes realizados com o Navegador Tor, o Wireshark não conseguiu localizar todos os Ips da cadeia criada, impossibilitando, assim,a localização do site que foi acessado.Relatos recentes, informam que há estudos e testes que estão conseguindo, aos poucos, quebrar a rede de camadas, criadas pelo Tor, para conseguirem localizar o IP de origem, mas ainda não se tem nada confirmado, apenas, relatos de ataques aos servidores do Tor. Um ponto que pode fazer com que os usuários não usem o Tor, é o fato de que para criação de todas as camadas, os acessos aos sites são um pouco mais demorados.

Com o Pidgin pode-se identificar que mesmo não usando a criptografia OTR, os pacotes são criptografados, o próprio Pidgin faz isto, dando sinais de aumento considerável de segurança. Nos testes com o ProtonMail pode-se perceber que, apesar de ser mais trabalhoso, todo o processo de decriptação do e-mail, torna-se bem mais seguro, pois o usuário pode ter certeza que somente quem tem a chave pode descriptografar o e-mail.

Durante o teste pôde-se observar uma grande melhoria na segurança do usuário, uma vez que não foram realizados testes exaustivos de todas as ferramentas. Porém, de uma forma geral, acredita-se que são eficientes, os recursos apresentados.

REFERENCIAS

ARRUDA, F. **PRISM:Zuckerberg nega participação do Facebook em programa secreto dos EUA**. Jun.2013. Disponível em: <http://www.tecmundo.com.br/privacidade/40639-prism-zuckerberg-nega-participacao-do-facebook-em-programa-secreto-dos-eua.htm>.Acesso em 18 de jun. 2015.

BALL, J; RUSHE, D. **NSA Prism program taps in to user data of Apple, Google and others**. Jun.2013. Disponível em: <http://www.theguardian.com>. Acesso em 25 de out. 2014.

CAMPI, M. **7 celebridades que tiveram a privacidade exposta na web.** Nov 2013. Disponível em:<http://info.abril.com.br/noticias/seguranca/fotonoticias/7-celebridades-que-tiveram-a-privacidade-exposta-na-web.shtml >. Acesso em 18 jun. 2015.

CASA CIVIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Acesso em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 18 de jun. 2015.

CULTURA DIGITAL. **Marco Civil da Internet em vigor**. jun.2014. Disponível em: <http://culturadigital.br>. Acesso em 23 de jun. 2014.

DIAS, T. **Marco Civil da Internet: política sem conexão**. 2013. Disponível em:<http://revistagalileu.globo.com>. Acesso em 25 de fev. 2015.

FOROUZAN, Behrouz; MOSHARRAF, Firouz. **FUNDAMENTOS DA CIÊNCIA DA CUMPUTAÇÂO**. São Paulo, 2011.

GREENWALD, Glenn. **Sem Lugar Para Se Esconder: Edward Snowden, a NSA e a espionagem do Governo Americano**. Nova York, 2014.

G1. **Ministério de Minas e Energia foi alvo de espionagem do Canadá**. Out 2013. Disponível em <http://g1.globo.com/politica/noticia/2013/10/ministerio-de-minas-e-energia-foi-alvo-de-espionagem-do-canada.html>. Acesso em 18 de jun. 2015.

G1. **Programa de vigilância dos EUA é suspenso temporariamente**. Jun.2015. Disponível em: <http://g1.globo.com/mundo/noticia/2015/06/programa-de-vigilancia-dos-eua-e-suspenso-temporariamente.html>. Acesso em 05 jun. 2015.

IBM. **Como funciona o SSL**. Disponível em <http://publib.boulder.ibm.com/tividd/td/TRM/GC32-1323-0/pt_BR/HTML/admin231.htm>. Acesso em 18 jun. 2015.

IX.BR. **Trafego**. Disponível em <ix.br>. Acesso em 18 de jun. 2015.

MACEDO, S. TO**P 5 - Invasão de Privacidade - Relembre 5 casos de celebridades exportas por hackers**. Set 2014. Disponível em: <http://f5.folha.uol.com.br/celebridades/2014/09/1509234-top-5---invasão-de-privacidade---relembre-5-casos-de-celebridades-expostas-por-hackers.shtml>. Acesso em 18 de jun. 2015

MORAES, R. **ProtonMail: e-mail criptografado contra o rastreamento da NSA é lançado**. May.2014. Disponível em: <http://www.tecmundo.com.br>. Acesso em 18 de mar. 2015.

OGLOBO. **'CitizenFour', vencedor do Oscar de melhor documentaria, teve cenas gravadas no GLOBO**. Disponível em: <http://oglobo.globo.com/cultura/filmes/citizenfour-vencedor-do-oscar-de-melhor-documentario-teve-cenas-gravadas-no-globo-15411515>. Acesso em 05 jun. 2015.

OGLOBO. **Edward Snowden ganha prêmio de liberdade de expressão na Noruega**. Atualizado jun.2015. Disponível em:<http://oglobo.globo.com/mundo/edward-snowden-ganha-premio-de-liberdade-de-expressao-na-noruega-16330414>. Acesso em 05 jun. 2015.

OTR. **Off-the-Record Messaging**. Disponível em: <https://otr.cypherpunks.ca/>. Acesso em 28 jan. 2015.

PIDGIN, **About Pidgin**. Disponível em: <https://www.pidgin.im/about/>. Acesso em 28 jan. 2015.

PIDGIN. **Pidgin 20.10.11**. Disponível em: <https://www.pidgin.im/>. Acesso em 28 jan. 2015.

PROTONMAIL. **About ProtonMail**. Disponível em <https://protonmail.ch/pages/about>. Acesso em 15 de fev. 2015.

TAILS. **Baixar, verificar e instalar**. Last Edit 26 Apr. 2015. Disponível em: <https://tails.boum.org/download/index.pt.html>. Acesso em 23 out. 2014.

TORPROJECT. **Tor: Overview**. Disponível em: <https://www.torproject.org/about/overview.html>. Acesso em 11 dez. 2014.

TORPROJECT. **What is the Tor Browser?**. Disponível em: <https://www.torproject.org/projects/torbrowser.html>. Acesso em 11 dez. 2014.

YOU GET SIGNAL. **Virtual Trace Route Tool**. Disponível em <http://www.yougetsignal.com/tools/visual-tracert/>. Acesso em 11 de jun. 2015.