FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Tecnologia em Segurança Da Informação

Luís Guilherme de Almeida

VIOLAÇÃO DE PRIVACIDADE

Uma Análise Sobre Coleta e Uso Indevido de Dados

Americana, SP

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Tecnologia em Segurança da Informação

Luís Guilherme de Almeida

VIOLAÇÃO DE PRIVACIDADE

Uma Análise Sobre Coleta e Uso Indevido de Dados

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Tecnologia em Segurança da Informação, sob a orientação do Professor Esp. Edson Roberto Gaseta

Área de concentração: Segurança da Informação

Americana, S. P.

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Almeida, Luís Guilherme de

A448v Violação de privacidade, uma análise sobre coleta e uso indevido de dados. / Luís Guilherme de Almeida. – Americana: 2016.

63f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Edson Roberto Gaseta

1. Segurança em sistemas de informação I. Gaseta, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Luis Guilherme de Almeida

VIOLAÇÃO DE PRIVACIDADE

Uma Análise Sobre Coleta e Uso Indevido de Dados

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 24 de junho de 2016.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
CEETEPS/Faculdade de Tecnologia – FATEC/ Americana

Daniele Junqueira Frosoni (Membro)
Especialista
CEETEPS/Faculdade de Tecnologia – FATEC/ Americana

Benedito Luciano Antunes de França (Membro)
Mestre
CEETEPS/Faculdade de Tecnologia – FATEC/ Americana

AGRADECIMENTOS

Em primeiro lugar à minha família, à minha amada esposa Isaina, às dezenas de mestres ao longo do curso, a todos da Agemcamp, em especial Maria Inês, Ester Viana e Luiz Bordin, por me apoiarem no momento mais difícil e doloroso de minha vida.

DEDICATÓRIA

A todo pobre de periferia que não desiste dos seus sonhos, não deixa de lutar pelo que é seu e não se deixa dominar pelo sistema.

“Se você tem algo que não quer que ninguém saiba, talvez você não deveria fazer isso em primeiro lugar”

(ERICK SCHMIDT – CEO *GOOGLE*)

RESUMO

O presente trabalho analisa os aspectos legais e técnicos envolvendo a violação da privacidade no ambiente virtual por meio da coleta indevida de dados, tendo como base processos movidos contra grandes empresas de tecnologia, como Microsoft, Google, Apple e Facebook, e também de documentação comprobatória de atividades ilegais por parte de empresas e governos, destacando os casos de espionagem do governo americano através da National Security Agency (NSA) e da agência britânica Government Communications Headquarters (GCHQ) com os respectivos programas de espionagem PRISM e TEMPORA, tendo sua existência sido revelada pelo ex agente da NSA Edward Snowden, com o vazamento de documentos secretos. Após esclarecidos os conceitos básicos sobre a coleta indevida de dados, parte-se para a fase de análise das políticas de dados e privacidade das empresas de tecnologias supracitadas e das legislações brasileira, americana e europeia, detalhando o funcionamento das operações de coleta e uso indevido de cada estudo de caso. Na próxima parte do projeto é realizado um experimento prático em um ambiente virtualizado utilizando o virtual box emulando uma rede doméstica e com a ferramenta de captura de pacotes de rede Wireshark para exemplificar como pode-se obter informações sobre o tráfego de rede de um usuário. Depois chegamos a parte em que são propostas medidas para mitigação da coleta indevida de informações como: bloqueio de *cookie*s, utilização de ferramentas que dificultem a violação dos direitos dos usuários de Internet e a adoção da ferramenta TAILS, um sistema operacional baseado em GNU/Linux que visa o anonimato e o sigilo de dados de seus usuários através da rede TOR, um tipo específico de ferramenta para navegação anônima. E por fim temos a conclusão discorrendo sobre os resultados obtidos com a elaboração deste trabalho e afirmando que não é possível que haja privacidade total em um mundo cada vez mais conectado, mas que há a possibilidade de mitigar os efeitos da vigilância em massa.

Palavras-Chave: Coleta indevida de dados; Privacidade na Internet; Espionagem digital.

ABSTRACT

This paper analyzes the legal and technical aspects involving the violation of privacy in the virtual environment through improper data collection, based on cases against large technology companies such as Microsoft, Google, Apple and Facebook, as well as supporting documentation illegal activities by companies and governments, highlighting the spying cases of the US government through the National Security Agency (NSA) and the British agency Government Communications Headquarters (GCHQ) with their spy programs PRISM and TEMPORA, and its existence was revealed by former NSA agent Edward Snowden with leaking secret documents. After clarified the basics of improper data collection, part to the analysis phase of data privacy policies and the companies above technologies and the Brazilian, American and European legislation detailing the operation of the collection and misuse operations of each case study. In the next part of the project is carried out a practical experiment in a virtualized environment using the virtual box emulating a home network and the Wireshark network packet capture tool to illustrate how one can obtain information about the network traffic of a user. Then we come to the part where measures are proposed to mitigate the improper collection of information such as blocking cookies, use tools that hinder the violation of the rights of Internet users and the adoption of TAILS tool, an operating system based on GNU / Linux which seeks anonymity and the confidentiality of data of its users through the TOR network, a specific type of tool for anonymous surfing. And finally we have the conclusion discussing the results obtained with the preparation of this work and stating that it is not possible to have complete privacy in an increasingly connected world, but there is the possibility of mitigating the effects of mass surveillance.

Keywords: improper collection of data; Privacy on the Internet; digital *spying*.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

INTRODUÇÃO

Com o conhecimento público dos casos de espionagem protagonizados pela *National Security Agency* (NSA) do *Government Communications Headquarters* (GCHQ) e dos conhecidos casos de processo contra grandes corporações sobre uso indevido de dados pessoais, vemos uma crescente necessidade de adotar mecanismos de proteção contra a violação do sigilo e de dados pessoais na Internet.

A capacidade de manter a privacidade no mundo digital, por vezes confronta-se com uma ameaça crescente e cada vez mais inerente a um mundo conectado em rede.

A necessidade voraz de empresas em coletar dados a respeito de perfis de consumo para maximizar os lucros de seus negócios ou a crescente preocupação de governos e agências de inteligência em saber quem, como, o quê, quando e por que está se realizando determinada ação na grande rede, abre espaço para uma discussão acalorada sobre até que ponto esta coleta de dados é lícita e com nosso consentimento? É possível manter a privacidade e o sigilo de nossos dados?

O objetivo geral do presente trabalho foi analisar as ações de empresas e governos que envolveram a coleta ou o uso indevido de dados dos usuários de Internet.

Os objetivos específicos foram detalhar casos relevantes e as técnicas utilizadas por empresas e governos para a coleta indevida de dados visando um melhor conhecimento delas.

Apontar erros e abusos por parte das organizações, baseado na legislação vigente, e apontar medidas de prevenção e mitigação da violação de privacidade.

O método científico de pesquisa utilizado foi de abordagem indutiva, qualitativa e quantitativa e de natureza pura.

Os procedimentos técnicos foram bibliográficos, documentais e experimentais, os dados foram obtidos através de observação e análise de conteúdo.

O trabalho foi estruturado em sete capítulos, sendo que o primeiro, introdutório, descreve a metodologia utilizada; O segundo conceitua alguns termos considerados importantes para o entendimento deste trabalho e discute alguns dos fatores que podem levar à vigilância e à coleta indevida de dados; o terceiro analisa os aspectos legais dos casos estudados; o quarto capítulo analisa os aspectos

técnicos de como funciona a coleta de dados; já no quinto, temos um experimento prático utilizando a técnica de captura de pacotes para comprovar a coleta de dados por parte de empresas como Facebook e Google; no sexto capítulo, propomos medidas para a mitigar e dificultar a coleta de dados, com base nas informações conseguidas a partir dos estudos realizados no capítulo anterior; o capítulo sétimo se reserva às considerações finais.

2 DEFINIÇÕES RELACIONADAS À COLETA INDEVIDA DE DADOS

É importante primeiro definirmos alguns termos que são considerados importantes, para que o conteúdo possa ser mais bem compreendido, são estes:

Confidencialidade: Um dos três pilares da segurança da informação, ela diz respeito à proteção que a informação deve possuir, a fim de permitir que apenas a pessoa com os devidos privilégios tenha acesso à determinada informação (ABNT, 2013b)[1].

Integridade: Outro pilar da segurança da informação, é referente à veracidade das informações em um determinado sistema, visa garantir que aquela informação é condizente com o que foi solicitado, que não há erros ou que não houveram adulterações nos dados (ABNT, 2013b).

Disponibilidade: O terceiro pilar da segurança da informação diz que o acesso à informação deve estar disponível sempre quando for solicitado, é importante manter mecanismos de redundância[2] e *backup*[3] para prevenir problemas (ABNT, 2013b).

Política de segurança: Plano que as organizações devem manter, seguindo as leis relevantes, orientando ações para evitar danos ao negócio devido a falhas de segurança, ela conta com normas e procedimentos que devem ser seguidos pelos colaboradores (clientes, funcionários e fornecedores) a fim de mitigar possíveis riscos aos sistemas de informação, como roubo de dados ou indisponibilidade dos sistemas (ABNT, 2013a).

Política de privacidade e uso de dados: Documento elaborado pelas empresas prestadoras de serviços, e aceitos pelos usuários, que definem como são coletadas, armazenadas, processadas e divulgadas as informações relacionadas aos usuários, geralmente fazem distinção entre informações públicas e privadas (ABNT, 2013a).

Coleta de dados: Ato de coletar informações dos usuários de determinada aplicação ou serviço eletrônico com os mais diversos propósitos, que, pode ser legal

---

[1] A norma em vigor até a data de publicação deste trabalho é a NBR ISO/IEC 27001:2013 que utiliza como referência normativa a norma ISO/IEC 27000.

[2] Redundância diz respeito à duplicação de determinado serviço ou sistema para que, em caso de falha do primeiro o segundo possa rapidamente assumir seu lugar.

[3] *Backup* é a ação de manter uma cópia segura dos dados caso os dados originais sofram algum dano.

ou ilegal de acordo com as leis do país do usuário e da instituição coletora e/ou de acordo com os contratos de privacidade.

Hacker: especialista em informática que utiliza seus conhecimentos avançados em Tecnologia da Informação para diversos propósitos, desde a criação da Internet e de sistemas colaborativos de código aberto[4] como o Linux, até a atos criminosos como roubo de senhas de cartão de crédito e terrorismo virtual, estes últimos conhecidos também por *crackers* (RAYMOND, 1998).

Cookie: De acordo com Tanenbaum (2003), Kurose e Ross (2010), são pequenos arquivos de texto, armazenados nos computadores dos usuários de navegadores *web* que são responsáveis por enviar dados aos servidores de *sites* quando o cliente solicita acesso, têm a finalidade de personalização e customização da navegação.

Pixel tag ou *web beacon:* são pequenos arquivos em formato de imagem, que redirecionam a navegação para servidores que contém código para rastrear navegação baseada em interesses e para o envio de *cookie*s (GEARY, 2012).

Criptografia: É o ramo da criptologia segundo Tanenbaum (2003), responsável pela transmissão segura de informações através de algoritmos[5] de cifras dos dados, de forma que somente emissor e receptor poderão compreender a mensagem enviada, geralmente envolve senhas e chaves de criptografia.

Big Data: De acordo com Henriques (2013), é um conceito tecnológico que se utilizada de ferramentas para a coleta, armazenagem, filtragem e geração de valor informacional da imensa massa de dados coletados nas diversas fontes geradoras, como as redes sociais e aplicativos para *smartphones* ou portais e que auxiliam na geração de perfis com informações detalhadas sobre determinado alvo com os mais diversos propósitos, desde a criação de campanhas publicitárias até a catalogação de terroristas em potencial.

[4]Código aberto refere-se ao tipo de licença de software, em que os usuários podem acessar, modificar e redistribuir os programas de acordo com suas necessidades e de maneira gratuita.

[5]Algoritmos são modelos matemáticos implementados em linguagem de programação capazes de solucionar problemas e automatizar tarefas.

2.1 VIGILÂNCIA EM MASSA E COLETA INDEVIDA DE DADOS

Segundo Foucault (*apud* GREENWALD, 2014) a necessidade de vigilância onipresente não apenas provê o aumento de poder das autoridades e a obediência da população como faz com que o indivíduo faça o que lhe é imposto apenas com a ideia de ser vigiado, um sistema eficaz de controle em que o controlado não perceba que está cumprindo o que lhe é imposto.

Por isto, que todo estado totalitário ou repressivo vai optar por utilizar de vigilância em massa contra seus cidadãos como sua principal arma de controle, e para que esta vigilância se torne efetiva é fundamental que haja uma coleta em massa de dados de todos os cidadãos e organizações que, por vezes, ocorre sem o devido consentimento e/ou secretamente.

Foucault (2004, p. 176) declara ainda que:

> [...] para se exercer, esse poder deve adquirir o instrumento para uma vigilância permanente, exaustiva, onipresente, capaz de tornar tudo visível, mas com a condição de se tornar ela mesma invisível. Deve ser como um olhar sem rosto que transforme todo o corpo social em um campo de percepção: milhares de olhos postados em toda parte, atenções móveis e sempre alerta, uma longa rede hierarquizada[...] E essa incessante observação deve-se acumular numa série de relatórios e de registros;[...] um imenso texto policial tende a recobrir a sociedade graças a uma organização documentária complexa.[...] o que é assim registrado são comportamentos, atitudes, virtualidades, suspeitas - uma tomada de contas permanente do comportamento dos indivíduos.[...]

Assustadoramente se analisarmos as palavras de Foucault veremos que este sistema de vigilância se assemelha muito com a Internet moderna, em que as redes sociais desempenham um papel crucial no fornecimento de todo tipo de informação a respeito dos usuários da rede.

As táticas de vigilância em massa e coleta de dados podem servir aos mais variados propósitos como o uso de *big data* para coletar informações sobre tendências de consumo e fazer assim, através de uma agressiva campanha midiática, que os consumidores desejem aquilo que lhes for imposto, mesmo antes que eles saibam que irão consumir aquele produto ou serviço, ou, por outro lado, o monitoramento de cidadãos para manter a ordem pública, ou classificar cidadãos como terroristas.

3 ASPECTOS LEGAIS DA COLETA INDEVIDA DE DADOS

A tecnologia e os problemas sociais e legais inerentes ao seu avanço possuem um ritmo de crescimento acelerado, dificultando a formulação e aplicação de leis específicas nesta área. A legislação brasileira relacionada aos problemas e questões no âmbito virtual nos permite da maneira possível, interpretar a violação de privacidade, a coleta e o uso indevido de dados.

3.1 LEGISLAÇÃO BRASILEIRA

O artigo 5º Inciso X da constituição de 1988 diz: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL,1988).

De acordo com o Marco Civil da Internet, lei 12.965/2014, define-se no “Art. 3º, Inciso II) proteção da privacidade; e III) proteção dos dados pessoais, na forma da lei; como princípios para a disciplina na Internet ” (BRASIL, 2014). Ainda em seu artigo 7º, Incisos I, II e III afirma-se que o acesso à Internet é essencial ao exercício da cidadania, a inviolabilidade da intimidade e vida privada e sigilo de suas informações armazenadas e do tráfego por ela gerado na rede, salvo por ordem judicial, são assegurados.

A obrigação por parte dos provedores de Internet de fornecer em seus contratos de prestação de serviços informações claras sobre o regime de proteção aos registros de conexão e acesso a aplicações de Internet é afirmada no inciso VI da lei de 2014; neste trecho por exemplo observa-se que as informações sobre a navegação dos usuários e o tempo em que permanecem conectados a determinada aplicação, não podem ser divulgadas, mas como veremos no capítulo X estas informações paradoxalmente são passíveis de coleta e armazenamento por agentes não autorizados.

Em seus Incisos VII e VIII do artigo 7º, o Marco Civil da Internet impede que os referidos dados acima sejam comercializados por provedores a terceiros, exceto por livre consentimento, expresso e informado de acordo com a lei; no entanto o que ocorre é que ao clicar em “aceito”, por vezes os consumidores estão concordando com o fornecimento de informações que eles nem imaginam que estão sendo

coletadas. Neste cenário o âmbito já não é mais de coleta ilegal, mas sim consentida, mesmo de maneira inconsciente, sob a influência de um termo de privacidade e uso de dados obscuro; há, todavia, os casos em que o indivíduo não é um usuário de determinada aplicação ou serviço e mesmo assim tem seus dados coletados e repassados a terceiros com os mais variados objetivos.

O Inciso X chama atenção sobre a exclusão definitiva dos dados fornecidos a uma aplicação da Internet e, neste ponto, o Marco Civil da Internet, toca em um ponto importante que foi um dos fatores que levou Maximillian Schrems, (IRLANDA 2015) a entrar com uma ação contra a Comissão para a proteção dos Dados, no qual alega a violação das leis de proteção de dados.

O artigo XI da legislação brasileira diz: “publicidade e clareza de eventuais políticas de uso dos provedores de conexão à Internet e de aplicações de Internet ” (BRASIL, 2014). Sobre este trecho é necessário citar que, para um usuário comum da Internet, as políticas de uso de dados e privacidade são, muitas vezes, documentos extensos e de difícil leitura, que não são orientados a uma fácil localização das informações neles contidas.

Ainda segundo Marco Civil da Internet (Brasil, 2014) no “Art. 8º, A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet. ”

Visto que a Constituição de 1988 e o Marco Civil da Internet prezam pela privacidade e inviolabilidade dos dados, ações que violam estes princípios como os revelados por Edward Snowden, ex-agente da NSA, originaram uma Resolução do Comitê Gestor da Internet no Brasil (CGI), condenando a violação dos direitos básicos da cidadania que claramente foram violados (CGIB, 2013).

Após os escândalos do vazamento de informações, com revelações de coleta ilegal de dados e programas de vigilância em massa foi realizado um estudo sobre o assunto e de acordo com a Anistia Internacional (2015), entrevistando 15 mil pessoas em 13 países, constatou-se que 80% dos brasileiros são contra interceptação e armazenamento de dados pelo governo americano. E que 65% dos brasileiros, 69% dos alemães e 67% dos espanhóis são contra a implementação, em seus respectivos países, de sistemas de vigilância dos dados de usuários na Internet.

A pesquisa demonstra ainda que 78% dos entrevistados acham que empresas como Facebook, Google, Microsoft e Apple devem adotar medidas para que governos não tenham acesso aos dados particulares.

Foi considerado neste trabalho de conclusão que a coleta indevida de dados pode ocorrer por parte de empresas contra cidadãos e vice-versa, governos contra cidadãos e vice-versa, governos contra governos, governos contra empresas e vice-versa.

3.2 POLÍTICAS DE DADOS E PRIVACIDADE DAS EMPRESAS

A política de privacidade e uso de dados das empresas de tecnologia como citadas anteriormente, são documentos elaborados a fim de esclarecer como são tratados os dados dos usuários, e que para ter efeito devem ter o aceite por parte do cliente.

Abaixo foram citados alguns exemplos de políticas de dados e privacidade analisados:

O Portal do CGI, órgão responsável pela gestão da Internet no Brasil, tem uma política de dados clara e objetiva, nela podemos observar que os dados dos usuários não são repassados a terceiros, porém como na maioria dos sites há *plug-ins* sociais incorporados como Youtube, Facebook e Twitter o que pode fazer com que *cookie*s ou *pixels* sejam enviados para os respectivos domínios desses *plug-ins.*

O documento ainda afirma:

> O site do Registro.br fornece alguns dados dos titulares de domínios que podem ser consultados apenas para fins de contato, ou ainda, para pesquisas de blocos de endereço, sendo terminantemente proibida a distribuição, transformação, modificação, comercialização e reprodução destas informações, em particular para fins publicitários ou similares. Se for comprovada qualquer forma de utilização indevida ou coleta abusiva dos dados dos titulares de domínios ‘.br ’, o NIC.br poderá, sem prévio aviso, impor uma restrição de acesso, sem prejuízo de serem adotadas medidas legais para punição deste ato (CGIB, 2015, p. 2).

A política de dados do Portal Terra, por exemplo, possui instruções de como não ter seus dados coletados pelo portal e se o usuário navegar sem ter realizado algum desses procedimentos, considera-se que está autorizando a empresa e seus parceiros a coletar esses dados (PORTAL TERRA, 2016). São elas a navegação

anônima, desativação de *cookie*s e uma prática chamada *opt-out*[6]*,* que consiste em solicitar que seus dados não sejam coletados por empresas parceiras.

Sites como o g1, do Grupo Globo, utilizam-se de *cookies* próprios, e também de terceiros; estes não sendo cobertos por sua política de dados (GRUPO GLOBO, 2015), e afirmando que repassam determinadas informações a parceiros, informando também sobre a desativação dos *cookie*s para evitar a coleta destes dados.

O mesmo ocorre com o Portal UOL, há também um trecho que diz: “Em hipótese alguma, serão coletados dados pessoais por terceiros sem anuência dos usuários” (PORTAL UOL, 2016). Porém, como será visto mais adiante no experimento prático é verificada coleta por parte de terceiros.

Política de dados e privacidade Google: A questão aqui é como manter a privacidade ante a Google, pois seus serviços tornaram-se indispensáveis ao uso da Internet, e é bem provável que em nível de usuário doméstico, ao navegar na Internet usando um *smatphone*, vendo um vídeo ou em um portal de compras você estará utilizando tecnologia Google e obrigatoriamente teve de concordar com sua política de dados, com seus serviços de anúncios em praticamente todos os portais da Internet, a coleta de dados tem base legal para ocorrer, porém de acordo com a *Comission Nationale de L’informatique et des Libertés* (CNIL) (BÉLGICA, 2012), o cruzamento destes dados através dos vários serviços da Google é que podem levar a identificação dos usuários, ferindo as leis da União Europeia .

A política de dados do Facebook possui 6 páginas, e em todo o documento, sobre a coleta de dados através de *cookie*s ela possui apenas duas linhas que informam que o Facebook usa *cookie*s e recomenda a leitura da política de *cookie*s da empresa e ao ler a política de *cookie*s verificamos que sim, o Facebook (2016a) confirma que mesmo você não sendo usuário e não tendo uma conta nos serviços oferecidos pela empresa você também é monitorado se acessar sites que possuem *plug-ins* sociais e/ou permitem que empresas parceiras do Facebook enviem *cookies* ao navegador do usuário, com o objetivo de oferecer propaganda direcionada; o que indica que mesmo você não concordando com a política de dados da empresa

[6]Pedido de interrupção de envio de cookies e propaganda direcionada, procedimento que solicita às empresas que retirem o cliente de sua base de dados e que deixem de coletar ou enviar informações ao usuário.

Facebook, ela aplica essa pratica de coletar dados indiscriminadamente a todos os usuários da internet com a justificativa de fornecer segurança, customização e melhores serviços.

Esta prática fere o Artigo 7º do Marco Civil da Internet (BRASIL, 2014) parágrafos 7º e 9º, que afirma que os dados só podem ser coletados e divulgados a terceiros por meio de consentimento livre, expresso e informado.

3.3 ESTUDOS DE CASO DE COLETA INDEVIDA DE DADOS

Casos de violação dos direitos dos usuários de internet, de escândalos de espionagem e vigilância em massa são noticiados com frequência na mídia, foram selecionados alguns desses casos para análise.

3.3.1 FACEBOOK

De acordo com a Comissão para a Proteção da Privacidade (BÉLGICA, 2015) o Facebook feriu as leis de proteção à privacidade de dados dos usuários de Internet na União Europeia, ao coletar dados de pessoas que não eram usuárias da rede social através de *plug-ins* sociais incorporados em outros portais, como por exemplo os botões “compartilhar”, “curtir” e “comentar” que estão presentes em milhões de portais ou *blogs,* como ficou comprovado no estudo encomendado pela comissão belga, conexões com os servidores do Facebook eram solicitadas e abertas no navegador do usuário sem seu conhecimento prévio, o que no entender da Comissão para a Proteção da Privacidade é uma prática ilegal.

Ao visitar uma página, se a mesma estiver sob um dos domínios do Facebook, é enviado ao navegador um *cookie,* que nada mais é que um pequeno arquivo de texto com informações sobre a navegação, com isto há a possibilidade de monitorar as preferências e perfis dos usuários. Mesmo que o usuário não tenha interação com recurso algum da rede social ou o botão curtir, por exemplo, este *cookie* é enviado de volta ao Facebook. Como está escrito na Recomendação nº4/2015 da Comissão belga, todo o monitoramento que não for previamente avisado ou solicitado pelo usuário é ilegal, sendo, portanto, o Facebook notificado nesta Recomendação a adotar medidas para interromper as ações de coleta

indevida (BÉLGICA, 2015).

Aos administradores dos portais que possuem os *plug-ins* sociais, foram recomendadas ações para adequação de seus sites de acordo com as leis de proteção de dados da União Europeia.

No documento foram citadas medidas a serem adotadas pelos usuários, como adição de aplicativos específicos no navegador para aumentar o nível de proteção contra a coleta de dados, a navegação em modo anônimo e a opção de não ter seus dados coletados por empresas que coletam *cookies* para oferecer propaganda baseada nos interesses dos usuários. Os internautas deveriam acessar o site da organização *Your Online Choices*[7] e realizar o *opt-out,* ou simplesmente deixar de utilizar a rede social se não quiser ser monitorado.

Nos Estados Unidos, por exemplo, Matthew Campbell e Michael Hurley, entraram com uma ação contra o Facebook, alegando a coleta e divulgação de dados enviados por meio de comunicação privada no *chat in box.* Neste caso os reclamantes realizaram testes que comprovaram que *links* compartilhados de maneira privada eram contabilizados como "curtidas" ou "*likes"* pelos portais que possuíam *plug-ins* sociais, prática esta que não estava claramente descrita na política de dados da empresa (CALIFÓRNIA, 2013).

Um dos casos mais notórios foi o processo aberto por Maximillian Schrems contra a Comissão Irlandesa de Proteção de Dados, em que o mesmo alega que os cidadãos da União Europeia não possuíam garantias da proteção de seus dados, que eram enviados para os Estados Unidos e em particular para o Facebook*,* sob a justificativa de invalidez do acordo 2000/520, conhecido como princípio de Porto Seguro (IRLANDA, 2015).

Devido às revelações de Edward Snowden sobre a coleta massiva de dados de cidadãos americanos e de outras nacionalidades, Schrems decidiu entrar com o processo pedindo que fossem adotadas medidas para impedir o envio e o acesso indevido de dados de cidadãos europeus que trafeguem para fora da Europa (IRLANDA, 2015).

[7]http://www.youronlinechoices.eu/

3.3.2 GOOGLE

A Google esteve envolvida em vários casos de coleta ou uso indevido de dados, mencionaremos aqui os casos *Google Wallet* (CALIFÓRNIA, 2015), ocasião em que a empresa foi acusada de vender a terceiros dados sigilosos de clientes, que utilizavam a plataforma para o pagamento de serviços como a compra de *Apps*[8] na *Play Store*.

De acordo com a juíza do caso, a empresa teria que enfrentar as acusações da reclamante, que alega ter seus dados como endereço, endereço postal, *e-mail* e telefone enviados desnecessariamente à Ycdroid, uma empresa de desenvolvimento de *Apps*, na ocasião em que ela pagou U$ 1,77 por um aplicativo de *e-mail,* violando assim uma lei de defesa dos consumidores da Califórnia (CALIFÓRNIA, 2015).

Outro exemplo é o caso do *Google Street View,* em que cidadãos americanos processaram a empresa alegando a coleta de informações críticas de redes Wi-Fi pelo veículo que realizava a gravação das imagens nas localidades (CALIFÓRNIA, 2010).

Semelhante ao caso americano o CNIL denunciou uma série de irregularidades cometidas pela Google em relação à coleta de informações de redes *wireless* e por não esclarecer o propósito da coleta destes dados, o cruzamento de informações de vários serviços e *Apps,* podendo levar a identificação pessoal do usuário e o tempo de armazenamento das imagens coletadas pelo Street View, este último violando o direito ao esquecimento (BÉLGICA, 2012). O documento menciona, por exemplo, que os objetivos dessas práticas não estavam claramente descritos na política de privacidade.

3.3.3 MICROSOFT WINDOWS 10

O Sistema Operacional da Microsoft está envolvido em polêmicas desde seu lançamento por causa de novos recursos, que segundo Microsoft (2016) coleta diversos dados privados dos usuários, através de tecnologias como o assistente pessoal Cortana*,* o buscador Bing e o serviço de armazenamento em nuvem

[8] Aplicativos para dispositivos móveis

OneDrive, os dados coletados incluem interesses e favoritos, nome e dados de contato: e-mails, endereços postais, números de telefone, etc.; além de credenciais, senhas, dicas de senhas e informações de segurança utilizadas na autenticação de contas; bem como dados demográficos, sexo, país, idade, língua; Dados financeiros: número do cartão de crédito, código de segurança; dados de uso, informações sobre o seu dispositivo em relação ao uso dos serviços, informações sobre a rede que o usuário utiliza, endereço IP (Internet Protocol), IMEI[9] de telefones, chaves de produtos instalados, etc.; dados de localização e todo o conteúdo produzido pelo usuário e que trafegue por qualquer serviço Microsoft. Ainda de acordo com a política de dados, essas informações podem ser repassadas a parceiros comerciais.

Há neste Sistema Operacional as opções de desativar a coleta de dados, porém alguns dados continuarão a ser captados dependendo do serviço utilizado, como prova Bright (2015), afirmando que mesmo configurando o Sistema para parar de coletar e enviar dados para a Microsoft, ainda assim foi possível monitorar o envio destes dados aos servidores da Empresa.

Há também o caso da Agência de Advogados Russos Bubnov and Partners que entrou com uma denúncia ao Procurador Geral da República Yury Chaika, alegando que o Windows 10 espiona os usuários, solicitando a proibição do uso do sistema operacional no país (THE MOSCOW TIMES, 2015).

Esta prática do Windows 10 não é muito diferente do que já ocorre com as ferramentas da Google e Facebook. A questão, no entanto, é que esta coleta realizada pelo Windows pode não ser ilegal, pois os usuários deste sistema Operacional aceitam os termos para poderem utilizá-lo, a questão é para qual propósito, ou, se a Microsoft e seus parceiros comerciais garantem a proteção e idoneidade do uso destas informações, haja visto que existem tecnologias capazes de capturar esses dados críticos.

[9]Número de registro composto por sequência numérica única que identifica o aparelho, não há dois aparelhos com o mesmo IMEI.

3.3.4 APPLE, DA VINCI, SHADY RAT, MIT

A Coréia do Sul, segundo o jornal o Globo (CORÉIA..., 2011), foi o primeiro país a multar a Apple por coletar dados de localização dos usuários de *IPhone* e *IPad.*

Allan e Warden (2011), por exemplo, realizaram um teste que mostra as informações de localização armazenadas pelos aparelhos. A empresa enfrentou posteriormente a esta decisão outros processos coletivos, tanto na Coréia do Sul quanto nos Estados Unidos.

Segundo Galli (2015) a empresa italiana de tecnologia Hacking Team teve um total aproximado de 400 Gigabytes de informações de seus bancos de dados divulgados por *hackers,* com informações sobre funcionários da empresa e seus clientes, além de clientes potenciais; e de acordo com o Portal Wikileaks, a Polícia Federal do Brasil teve interesse em contratar os serviços da empresa em 2014.

> De acordo com a ONG Repórteres sem Fronteiras, a empresa é 'mercenária digital' e considerada 'inimiga da Internet'. O sistema de controle remoto oferecido por eles, chamado Da Vinci, quebra criptografia de e-mails, arquivos e ligações telefônicas. Com o uso do software, é possível acessar câmeras e microfones de forma remota, gravar ligações e usar o teclado, além de rastrear o uso da Internet e a troca de mensagens (GALLI, 2015, p. 1).

Semelhante ao caso do programa Da Vinci, a operação Shady Rat, em um *white paper* publicado pela McAfee, revelou que 71 corporações entre empresas e governos foram vítimas, dentre elas os governos dos Estados Unidos, Taiwan, Coréia do Sul, Vietnã e Canadá, o Comitê Olímpico Internacional, várias empresas de material bélico e empresas de alta tecnologia, a suspeita, é a de que um agente estatal esteja envolvido por trás dos ataques (ALPEROVITCH, 2011).

> No caso da ONU, os hackers invadiram o sistema de computação de seu secretariado em Genebra, em 2008, e operaram em silêncio na rede durante dois anos, obtendo discretamente grande volume de dados sigilosos, de acordo com a McAfee (FINKLE, 2011, p.1).

E por fim temos um estudo do Massachucetts Institute of Technology (MIT), em que 500 aplicativos de *smartphones* Android foram analisados e segundo Ruby *et al* (2015), 46,2% de toda a comunicação realizada por estes aplicativos era oculta,

ou seja, sem o conhecimento do usuário e que muitas dessas informações não são vitais para o funcionamento e desempenho dos aplicativos.

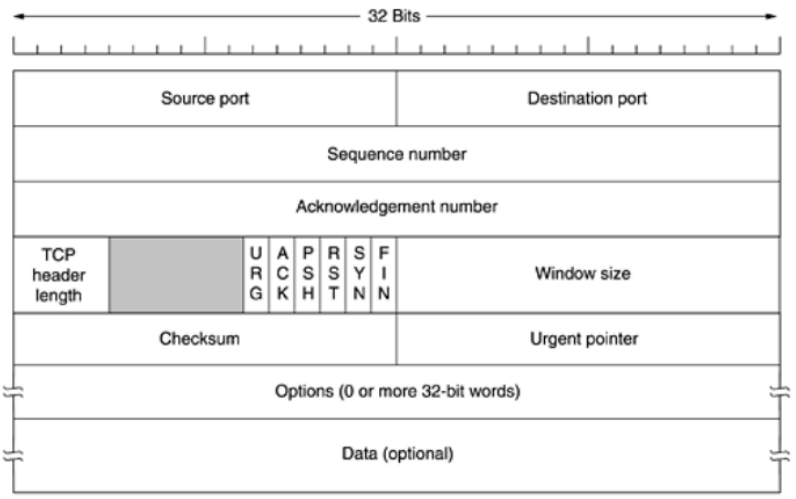
4 ASPECTOS TÉCNICOS DA COLETA INDEVIDA DE DADOS

Existem inúmeras técnicas para realizar a coleta de dados, para o caso da navegação *web,* vamos analisar o protocolo HTTP (Hipertext Transfer Protocol), os *cookies*, *pixels* e os *plug-ins* sociais.

4.1 TCP/IP

Em nosso estudo levamos em consideração como é feita a conexão entre um cliente e um servidor na *web* utilizando o Transmission Control Protocol (TCP); para isso analisamos o cabeçalho TCP e o protocolo HTTP.

Figura 1 - Cabeçalho TCP

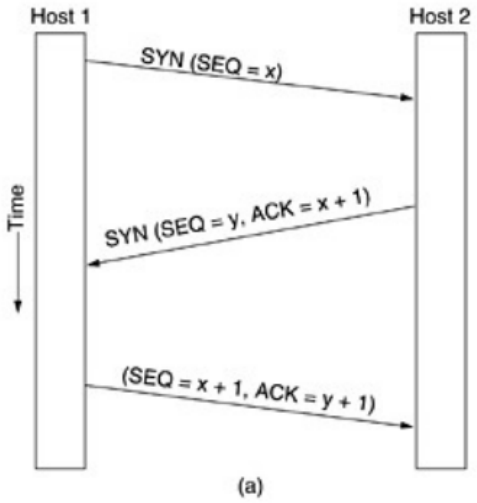


Fonte: Tanenbaum (2003, p. 408)

Os campos *source port* e *destination port* se referem às portas de origem e destino do pacote; o campo ACK é utilizado para confirmação do recebimento do segmento de dados do pacote e recebe os valores 0 ou 1; o campo SYN é utilizado para solicitar conexões, recebe os valores 1 e 0, ao enviar uma solicitação c*onnection request* os campos possuem valor SYN = 1 e ACK = 0, ao receber uma confirmação c*onnection accepted* os campos possuem valor SYN = 1 e ACK = 1; o campo ACK serve para diferenciar as duas possibilidades (TANENBAUM, 2003).

Os *bits* SYN e ACK foram importantes em nosso estudo porque através deles conseguimos identificar as conexões que estavam sendo recebidas e enviadas em nossos testes.

Figura 2 - Conexão TCP *Handshake*



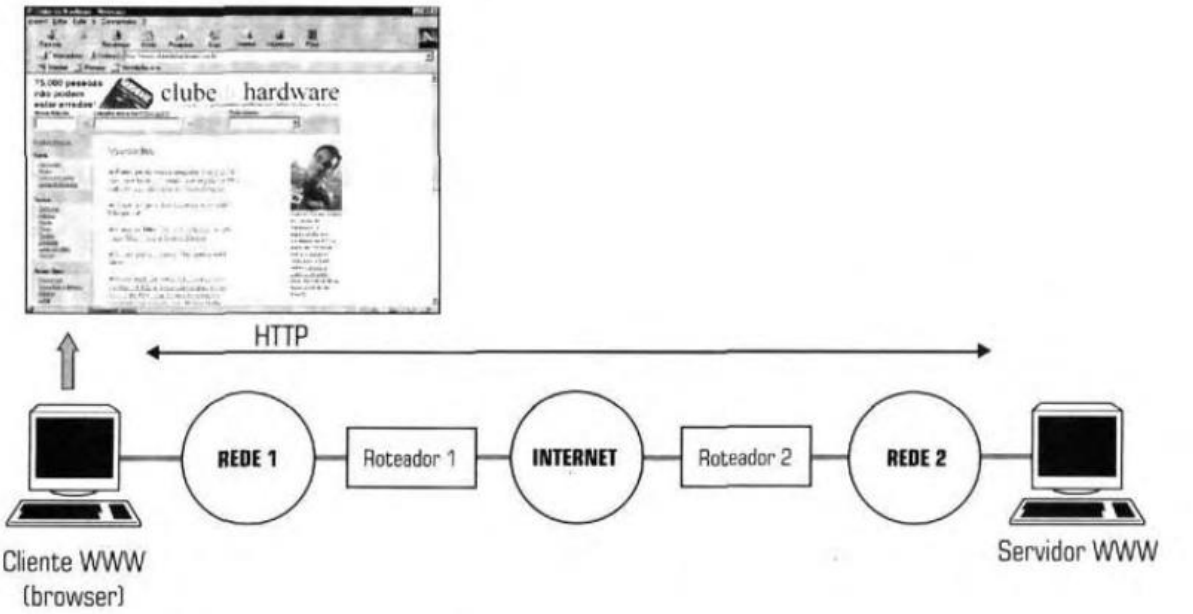
Fonte: Tanenbaum (2003, p. 411)

O processo de *handshake* funciona da seguinte maneira:

1) O cliente envia um bit SYN ao servidor; 2) o servidor que está ouvindo do outro lado reconhece o SYN e envia um SYN mais um ACK de confirmação; 3) o cliente envia a sequência seguinte e com um ACK para confirmar; 4) a conexão é estabelecida; 5) os dados são trocados; 6) para finalizar a conexão, o processo é o mesmo só que substituindo SYN por FIN.

Os navegadores utilizam o protocolo HTTP para fazer uma requisição de acesso a uma página em um servidor *web*, o protocolo TCP cria um *socket*, que funciona como um túnel de ligação entre as duas pontas, possuindo os endereços de origem e destino e as portas de origem e destino, no caso da *web* as portas 80 ou 443 (HTTPS) são abertas do lado do servidor (Tanenbaum, 2003), o protocolo HTTP possui diversos métodos, um desses métodos analisados por nós foi o GET que é utilizado para solicitar conexão.

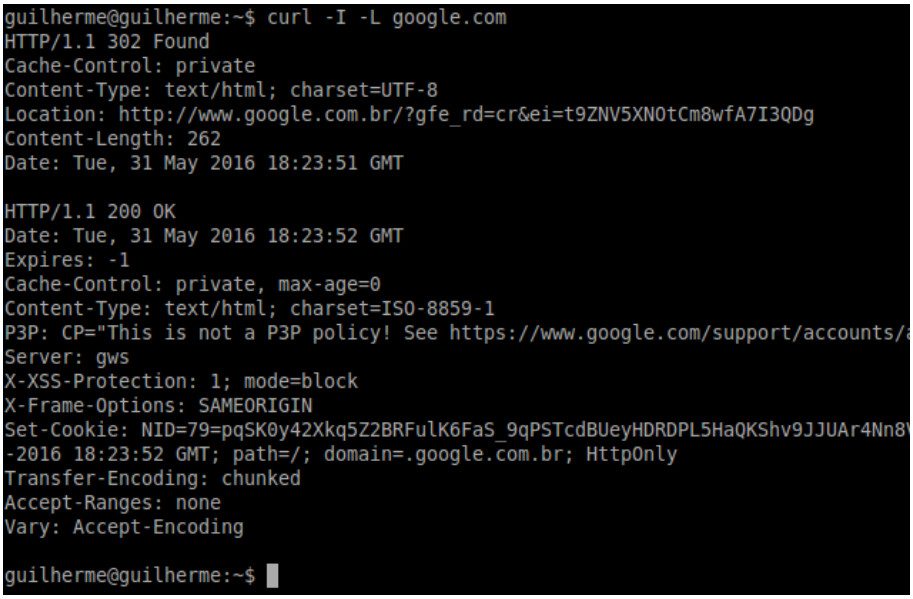
Figura 3 - Funcionamento do HTTP



Fonte: Torres (2001, p. 126)

O cabeçalho de mensagem set-cookie diz ao navegador para armazenar um *cookie* no computador. O cabeçalho *cookie* retorna ao servidor um *cookie* armazenado em uma conexão anterior, o cabeçalho host identifica o servidor de DNS (Domain Name Server) que é retirado da URL (Uniform Resource Locator) e o *server* traz informações sobre o servidor como tipo, versão, etc. (TANENBAUM, 2003), estes cabeçalhos foram úteis para identificar a origem e destino dos pacotes e determinar a coleta indevida de dados.

Figura 4 - Cabeçalho HTTP



Fonte: Autoria própria

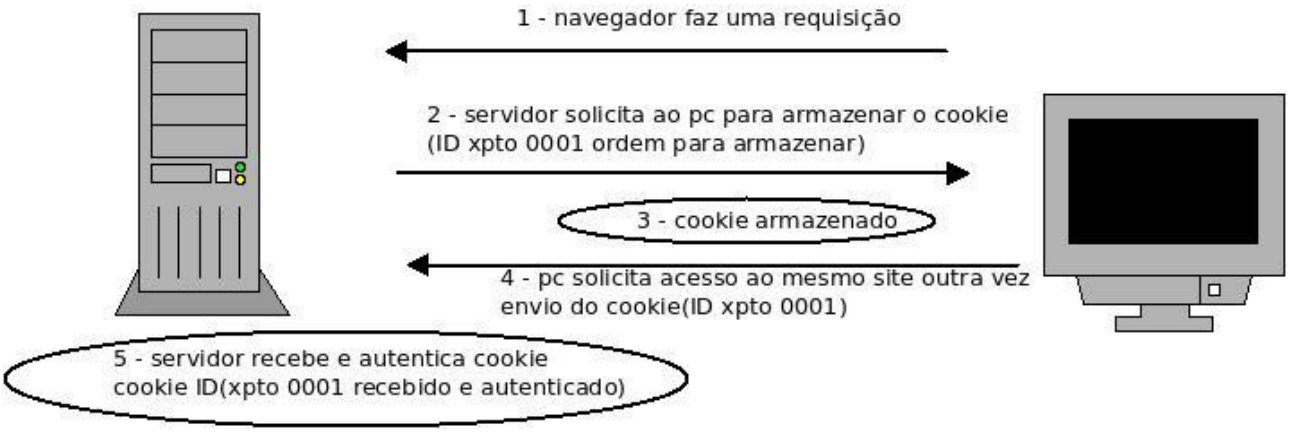
A imagem acima exibe as informações contidas em um cabeçalho HTTP após solicitarmos acesso ao site da Google.

4.2 *COOKIES*

O Protocolo HTTP 1.0 não mantinha um estado de conexão permanente, o que quer dizer que a cada solicitação que seu navegador fazia ao servidor acarretaria em uma nova requisição/resposta. Para resolver este problema foram criados os *cookies* pela Netscape.

Toda vez que uma página é acessada o servidor pede ao cliente que armazene um pequeno arquivo de texto no disco, assim toda vez que o cliente solicitar novamente acesso ele envia este *cookie* junto ao cabeçalho da solicitação para o servidor que irá reconhecê-lo e interpretar as informações nele contidas (TANENBAUM, 2003).

Figura 5 - Funcionamento de um *cookie*



Fonte: Autoria própria

Dessa maneira pode-se manter as informações de um carrinho de compras por exemplo ou suas preferências de navegação, se mudar de página ou fechar o navegador.

Os *cookies* em si não são perigosos pois são tratados como dados e não como programas, porém nada impede que algum *hacker* descubra alguma falha no navegador que explore *cookies*.

Segundo Barth (2011), na Request For Comments (RFC 6265), os *cookies* são compostos pelos campos:

Creation_utc = referente a data de criação.

Expires_utc = referente ao fim de sua validade.

Last_access_utc = data do último acesso.

Host_key = o domínio ao qual o *cookie* pertence.

Name = identifica o *cookie*.

Path = caminho onde é armazenado.

Value = conteúdo do *cookie*.

Encrypted value = conteúdo criptografado.

Figura 6 - Campos de um *cookie*

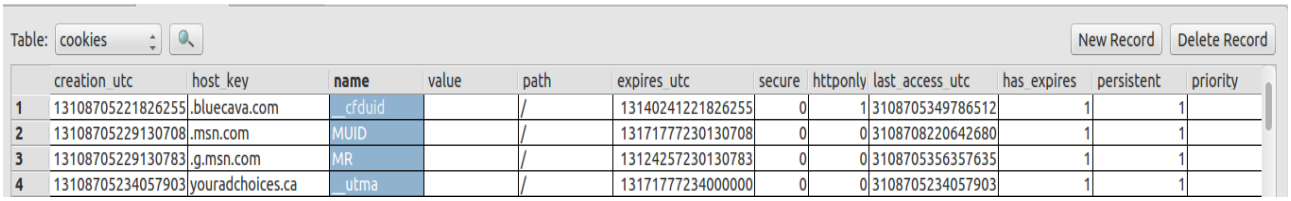


Table: cookies — New Record — Delete Record

	creation_utc	host_key	name	value	path	expires_utc	secure	httponly	last_access_utc	has_expires	persistent	priority
1	13108705221826255	.bluecava.com	__cfduid		/	13140241221826255	0	1	3108705349786512	1	1	
2	13108705229130708	.msn.com	MUID		/	13171777230130708	0	0	3108708220642680	1	1	
3	13108705229130783	.g.msn.com	MR		/	13124257230130783	0	0	3108705356357635	1	1	
4	13108705234057903	youradchoices.ca	__utma		/	13171777234000000	0	0	3108705234057903	1	1	

Fonte: Autoria própria

No caso do Google Chrome utilizado no Gnu/Linux, por exemplo, os arquivos ficam armazenados em */home/usuário/.config/google-chrome/Default/* e pode-se visualizar seu conteúdo com o aplicativo SQLite Database Browser.

4.3 *WEB BEACONS* OU *PIXEL TAGS*

As empresas descobriram o quão vantajoso pode ser coletar o perfil das pessoas que utilizam a Internet e exibir propaganda direcionada de acordo com seus interesses de navegação, por isso utilizam *pixel tags* ou *web beacons,* por exemplo.

O processo se inicia quando o cliente faz uma requisição a um portal e neste há várias imagens que o navegador vai baixar junto com o *cookie* do portal acessado. Suponha que a página fulano.com.br foi acessada, no código da página há um *link* para uma imagem, por exemplo www.xpto.com/00001.png, o cliente vai solicitar esta imagem ao servidor *web* e com ela virá um *cookie* da empresa de *marketing* xpto, esta empresa vai saber qual página foi acessada devido a imagem com o *id* 00001 estar relacionada a página fulano.com.br. Após entrar em outra página que contenha um pixel da xpto, o cliente vai associar o *id* de usuário do primeiro *cookie* a esta segunda requisição, assim a empresa xpto agora saberá duas páginas que foram acessadas. Com o passar do tempo a empresa consegue montar um perfil de interesses do usuário, estas informações, no entanto, não são suficientes para identificar o usuário, porém com o IP em mãos basta cruzar os dados com outro tipo de banco de dados, por exemplo, se o usuário preencher um cadastro com nome e endereço em um portal que tem parceria com a xpto, a empresa consegue agora vender seu perfil completo para outras empresas (TANENBAUM, 2003).

Essas imagens são da mesma cor do fundo e tem dimensões de 1x1 *pixel*, ou seja, são invisíveis e muitos pixels têm suas URL's redirecionadas para executar código JavaScript ou outra linguagem.

Figura 7 - Funcionamento de um *Pixel*

Fonte: Signal (2010-2016)

Na imagem acima podemos visualizar o funcionamento de um *pixel,* primeiro o navegador solicita uma página do servidor *web,* em seguida o servidor atende a solicitação enviando a página, e um *script*[10] criado por alguma empresa terceira de coleta de *cookies,* logo após o navegador executa este código e coleta os dados, estes são enviados para o servidor da empresa, e por fim o servidor envia um *cookie* baseado nas preferências de conteúdo, para ser armazenado na máquina do usuário.

[10] Código escrito em linguagem de programação de *scripts* que é interpretado e executado pelo navegador.

Figura 8 - Pixel do *Facebook*

Facebook pixel base code

```
<script>
!function(f,b,e,v,n,t,s){if(f.fbq)return;n=f.fbq=function(){n.callMethod?
n.callMethod.apply(n,arguments):n.queue.push(arguments)};if(!f._fbq)f._fbq=n;
n.push=n;n.loaded=!0;n.version='2.0';n.queue=[];t=b.createElement(e);t.async=!0;
t.src=v;s=b.getElementsByTagName(e)[0];s.parentNode.insertBefore(t,s)}(window,
document,'script','//connect.facebook.net/en_US/fbevents.js');
// Insert Your Facebook Pixel ID below.
fbq('init', '<FB_PIXEL_ID>');
fbq('track', 'PageView');
</script>
<!-- Insert Your Facebook Pixel ID below. -->
<noscript><img height="1" width="1" style="display:none"
src="https://www.facebook.com/tr?id=<FB_PIXEL_ID>&ev=PageView&noscript=1"
/></noscript>
```

Standard event code outside the Facebook pixel base code

```
<script>

fbq('track', 'ViewContent');

</script>
```

Fonte: Facebook (2016c)

A figura acima mostra como é o código base dos *pixels* do Facebook e que devem ser incorporados no código-fonte dos portais, na sexta linha do *script* podemos observar o trecho do comando que cria a conexão com os servidores da empresa: "(*window,document,'script','/connect.facebook.net/em_us/fbevents.js'*)".

4.4 PLUGINS SOCIAIS

A imensa maioria dos portais modernos possui algum tipo de *plug-in* das mais variadas redes sociais, como Facebook, Google Plus, Twitter, etc.

Ao incorporar o código de um *plug-in* em sua página, o portal pode monitorar as preferências dos usuários e desenvolver uma estratégia que lhe traga mais negócios ou visitantes, porém toda a atividade é também coletada e enviada aos servidores das empresas proprietárias destes *plug-ins*. O código embutido é carregado e executado toda vez que o usuário acessa uma página, geralmente contendo um *link* para o servidor onde está hospedado o código e em alguma linguagem de *script* como o PHP ou o JavaScript por exemplo.

As instruções que podem estar contidas nesses *plug-ins* incluem a criação e solicitação de envio de *cookies*, captura de reações a publicações, coleta de dados fornecidos em comentários, etc. O problema é que os *plug-ins* sociais coletam tanto

as informações dos usuários destas redes sociais quanto as de não usuários (ALSENOY, 2015).

Figura 9 - Código do botão curtir *Facebook*

```
</head>
<body>

        <!-- Load Facebook SDK for JavaScript -->
        <div id="fb-root"></div>
        <script>(function(d, s, id) {
          var js, fjs = d.getElementsByTagName(s)[0];
          if (d.getElementById(id)) return;
          js = d.createElement(s); js.id = id;
          js.src = "//connect.facebook.net/en_US/sdk.js#xfbml=1";
          fjs.parentNode.insertBefore(js, fjs);
        }(document, 'script', 'facebook-jssdk'));</script>

        <!-- Your like button code -->
        <div class="fb-like"
                data-href="http://www.your-domain.com/your-page.html"
                data-layout="standard"
                data-action="like"
                data-show-faces="true">
        </div>

</body>
</html>
```

Fonte: Facebook (2016b)

O código-fonte do *plug-in* social “curtir” do Facebook possui código que solicita conexão com os servidores da empresa, como pode ser visto na figura 9, com o trecho “*js.src* = "//connect.facebook.net/en_US/sdk.js#xfbml=1".

Figura 10 - Código do plug-in botão +1 da Google

```
<script src="https://apis.google.com/js/platform.js" async defer></script>
<g:plusone></g:plusone>
```

Fonte: Google (2015)

Semelhante fato ocorre com o *plug-in* “+1” da rede social *Google Plus*, figura 10.

Figura 11 - Código do *plug-in* Botão compartilhar do Twitter

```
<a class="twitter-share-button"
 href="https://twitter.com/intent/tweet?text=Hello%20world"
 data-size="large">
Tweet</a>
```

Fonte: Twitter (2016)

Na figura acima vemos o código do *plug-in* “compartilhar” do Twitter, de estrutura mais simples que os anteriores.

4.5 PRISM / TEMPORA

Após o vazamento de documentos sigilosos da NSA pelo ex-agente Edward Snowdem, foi revelada a existência de uma avançada estrutura de monitoramento, armazenagem e coleta indevida de dados não só de usuários, mas também de grandes corporações de tecnologia e órgãos governamentais de vários países, tanto os considerados inimigos como os considerados aliados.

Nos documentos haviam trechos afirmando que:

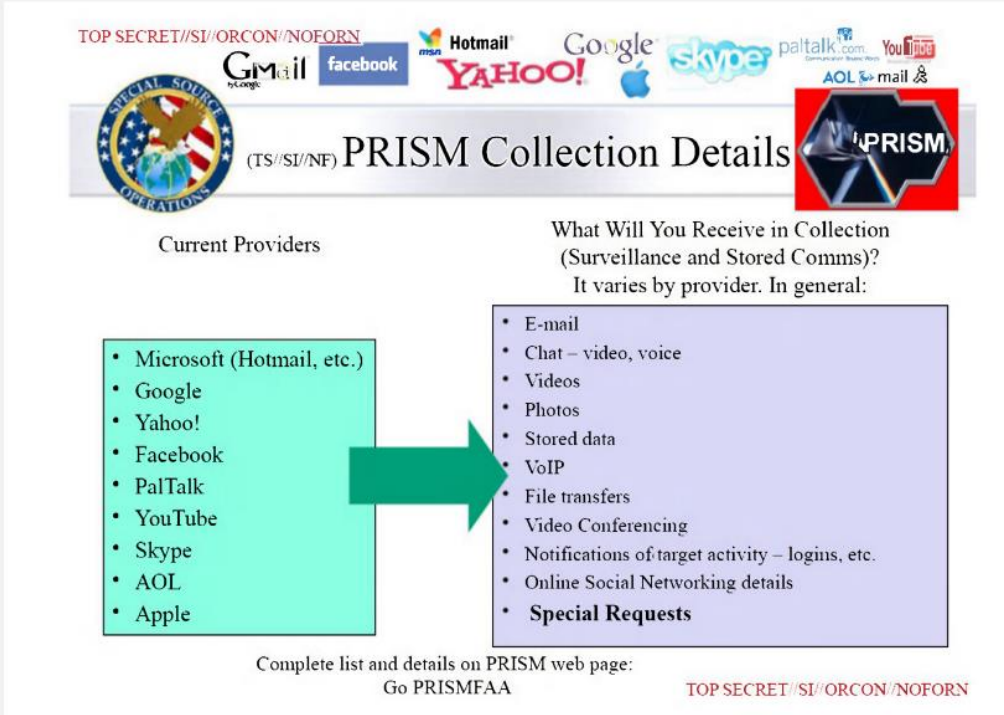
> No período de um mês a partir de 8 de março de 2013, por exemplo, um slide do BOUNDLESS INFORMANT mostrava que uma única unidade da NSA, chamada Global Access Operations (Operações de Acesso Global, GAO na sigla em inglês), tinha coletado dados sobre mais de 3 bilhões de chamadas telefônicas e e-mails que haviam transitado pelo sistema de telecomunicações norte-americano.
> (‘DNR’, ou ‘Dialed Number Recognition’, ‘reconhecimento de número discado’, refere-se a chamadas telefônicas; ‘DNI’, ou “Digital Network Intelligence”, inteligência de rede digital”, refere-se a comunicações feitas via Internet, como e-mails.) Esse número excedia coletas nos sistemas da Rússia, do México e de quase todos os países da Europa, e equivalia mais ou menos ao total de dados coletado na China.
> No geral, em apenas trinta dias, a unidade coletara dados sobre mais de 97 bilhões de e-mails e 124 bilhões de chamadas do mundo inteiro. Outro documento do BOUNDLESS INFORMANT oferecia detalhes dos dados coletados em um único período de trinta dias na Alemanha (500milhões), Brasil (2,3 bilhões) e Índia (13,5 bilhões). Outros arquivos mostravam, ainda, a coleta de metadados em parceria com os governos francês (70 milhões), espanhol (60 milhões), italiano (47 milhões), holandês (1,8 milhão), norueguês (33 milhões) e dinamarquês (23 milhões) (GREENWALD, 2014, p 73).

Segundo Greenwald (2014), PRISM é o nome dado ao programa de vigilância em massa da NSA, que utiliza de diversas estruturas como a Ghostmachine (GALLAGHER, 2014), uma infraestrutura analítica de *Big Data* para o armazenamento e processamento de dados em nuvem utilizada pelo programa PRISM e outros serviços de monitoramento em massa.

O PRISM se utiliza também do XKeyscore uma rede de servidores espalhados pelo mundo utilizada para processamento e armazenamento das informações coletadas pelas diversas organizações envolvidas com rastreio, monitoramento e armazenagem dos dados de pessoas e organizações (GREENWALD, 2013).

O Tempora é Similar ao programa PRISM, só que pertencente ao GCHQ (MACASKILL *et al*, 2013).

Figura 12 - Empresas envolvidas com o PRISM



Fonte: NSA… (2013)

Na figura 12, podemos ver a relação de empresas envolvidas e o tipo das informações fornecidas para o PRISM, de acordo com os *slides* secretos revelados pelo ex-agente da NSA, Edward Snowden (NSA..., 2013).

As técnicas de coleta principais, segundo Greenwald (2014), eram a interceptação de cabos submarinos intercontinentais, a coleta de informações de servidores de grandes empresas de tecnologia e a infecção de alvos específicos com um *malware* denominado “inserção quântica” em um total de mais de 100.000 computadores invadidos, na figura 13 abaixo, os alvos infectados estão em amarelo.

Figura 13 - Mapa com os alvos infectados pelo *malware da* NSA

Fonte: Greenwald (2014, p. 101)

Um grupo composto por 5 países de língua inglesa, Estados Unidos, Grã-Bretanha, Canadá, Austrália e Nova Zelândia denominado “Os cinco Olhos” (The Five Eyes), compõe a força tarefa na operação desta rede de monitoramento, porém há categorias de informações que somente os Estados Unidos têm acesso (GREENWALD, 2014).

5 MONITORANDO A COLETA DE DADOS COM WIRESHARK

O seguinte experimento foi realizado com o propósito de observar atividade suspeita que pode estar relacionada com a coleta indevida de dados por parte das empresas supracitadas, com ênfase no Facebook, utilizando-se da captura de pacotes do protocolo TCP/IP.

Ferramentas: Sistema operacional Linux Lubuntu 14.04, farejador de tráfego de rede Wireshark os comandos *nslookup* e *whois*.

5.1 IDENTIFICANDO IP'S A SEREM ANALISADOS

Procedimentos: O primeiro passo foi determinar lista de IP´s relacionados com os alvos a serem investigados, no caso deste trabalho: Facebook e Google.

Para isso foi executado o seguinte comando no terminal:

Figura 14 - Comando nslookup

```
nslookup facebook.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   facebook.com
Address: 173.252.91.4
```

Fonte: Autoria própria

Após descobrir o IP do alvo, realizamos uma consulta whois, com o seguinte comando:

Figura 15 - Consulta whois

```
guilherme@guilherme:~$ whois -h whois.radb.net 173.252.91.4
route:      173.252.64.0/19
descr:      facebook, inc.
origin:     AS32934
mnt-by:     MAINT-AS32934
changed:    phoose@fb.com 20111006  #17:54:39Z
source:     RADB
```

Fonte: Autoria própria

De posse do código do servidor de DNS que no exemplo da figura 15 é AS32934 executamos uma nova consulta *whois*:

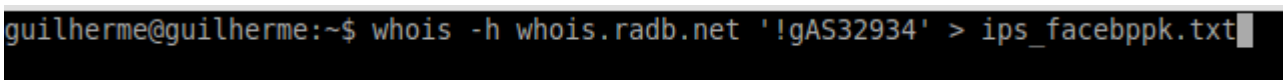
Figura 16 - Criação de um filtro de IP's do *Facebook* para o Wireshark

Fonte: Autoria própria

A nova consulta retornou todos os endereços de servidores relacionados ao *Facebook*.

O seguinte trecho do código que aparece na figura 17 redireciona o resultado da nova consulta *whois* para o arquivo ips_*Facebook*.txt:

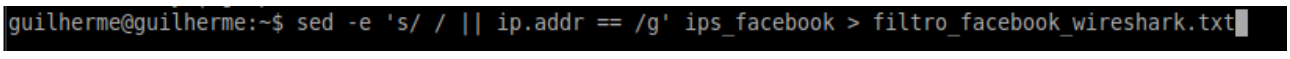
Figura 17 - Saída do comando *whois* para o arquivo de IP's do *Facebook*



Fonte: Autoria Própria

E o comando *sed*:

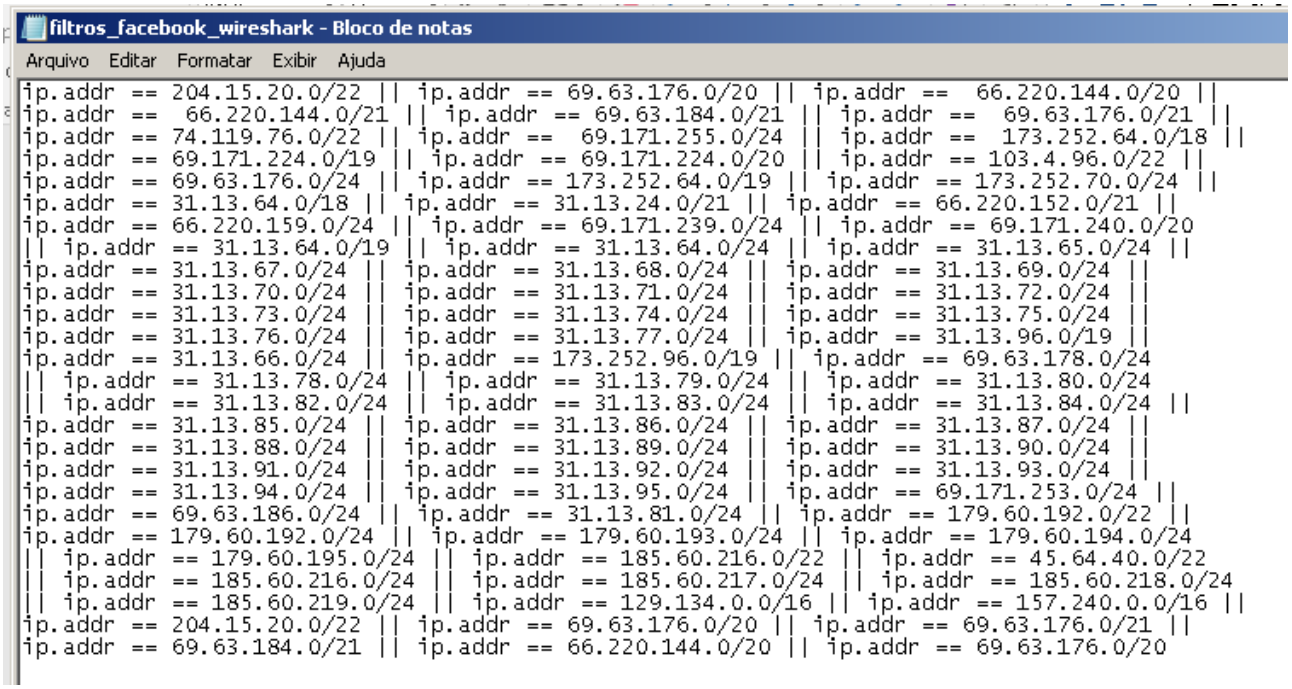
Figura 18 - Comando sed para ordenar os IP's do *Facebook*



Fonte: Autoria própria

Cria um filtro para o Wireshark com o seguinte conteúdo:

Figura 19 - IP's relacionados ao *Facebook*



Fonte: Autoria Própria

Realizamos os mesmos procedimentos com o domínio *Google.com*, porém como a consulta *whois.radb.net* retornou uma lista de IP's muito extensa, foi simplificado o filtro, optando então por criar um arquivo usando a saída do comando *whois* com um número suficiente de IP's para poder realizar os testes.

5.2 TESTE: NAVEGAÇÃO EM MODO NORMAL

O primeiro passo foi limpar o cache dos navegadores Firefox e Chrome para evitar contaminar a pesquisa com *cookie*s antigos.

Procurou-se na pesquisa buscar na Internet por termos polêmicos que, poderiam traçar um perfil de usuário, os termos foram: *AIDS, câncer, pedofilia, atentado terrorista, presidente Obama, terrorismo, homem bomba,* palavras estas que poderiam ser associadas, por exemplo, a um terrorista pedófilo, ou um paciente terminal com planos de assassinar o presidente.

Determinamos também duas categorias de portais a serem analisados:

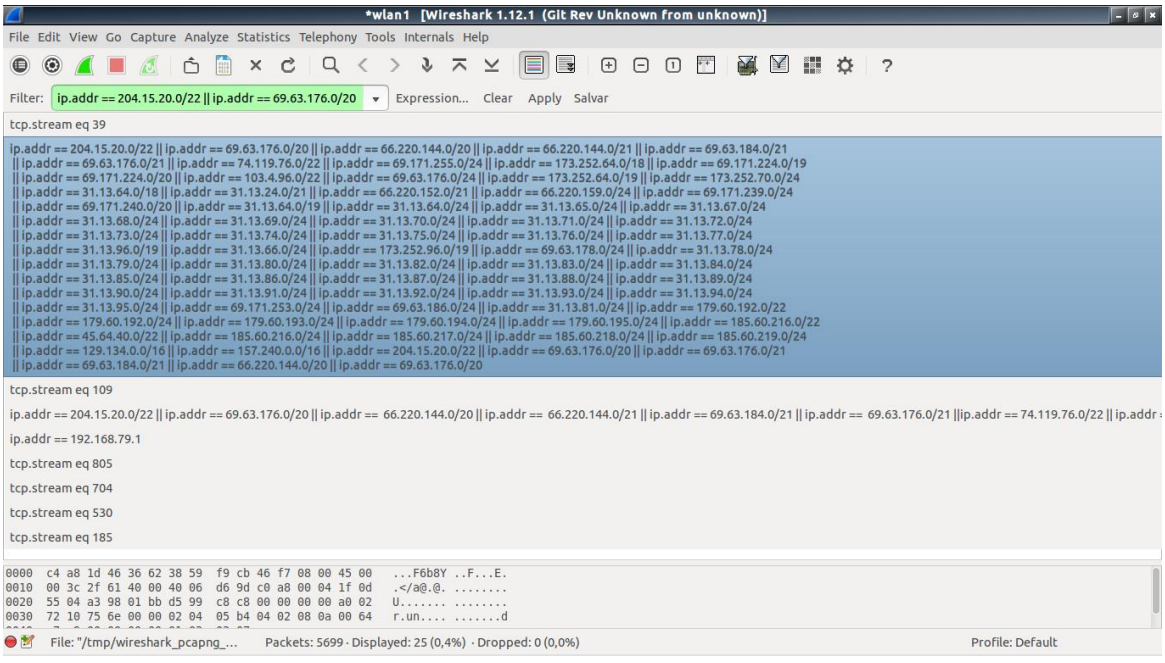
Sites simples: aqueles que não possuem *plug-ins* sociais nem outros recursos que possam coletar dados, exemplo: ftp.unicamp.br, gnu.org, pudim.com, etc. Estes com pouca ou nenhuma coleta de dados por empresas terceiras, envio e/ou recebimento de *cookie*s e solicitações de conexão do Google e Facebook.

Sites elaborados: uol.com.br, g1.com.br, terra.com.br, bbc.com.br, etc.

Estes portais por possuírem as tecnologias que permitem monitoramento foram analisados com mais cautela, pois realizamos uma navegação em modo normal e sem desabilitar os *cookie*s pelos portais citados, evitando acessar o *Facebook*.com, utilizando o buscador da Google e o buscador DuckDuckGo nos navegadores Firefox e Chrome, utilizamos o Lynx[11]também.

O *Wireshark* foi ativado para capturar os pacotes que trafegavam na rede no momento da navegação, analisando o histórico logo em seguida, foi observado que não havia registro do Facebook, partiu-se então para a análise dos pacotes, aplicamos o filtro de IP's do Facebook no Wireshark, o filtro aplicado como visto na figura 20 retornou os pacotes que possuíam alguma ligação com IP's do domínio Facebook.com.

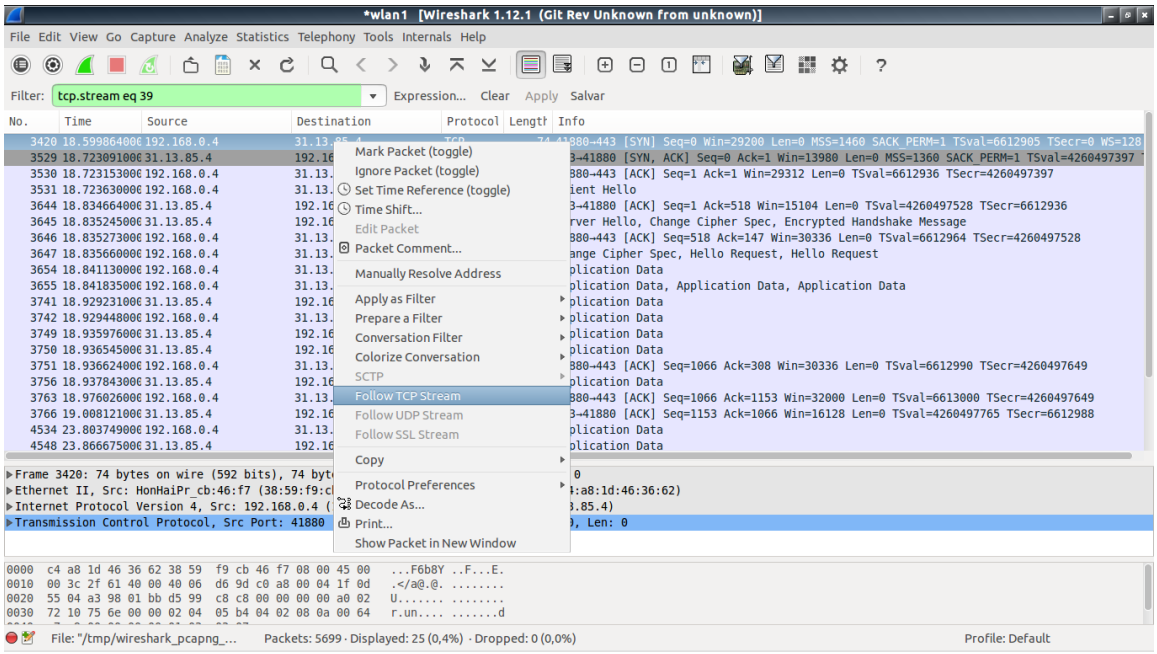
Figura 20 - Aplicando filtro de IP's do *Facebook*



Fonte: Autoria própria

[11] Navegador em modo texto.

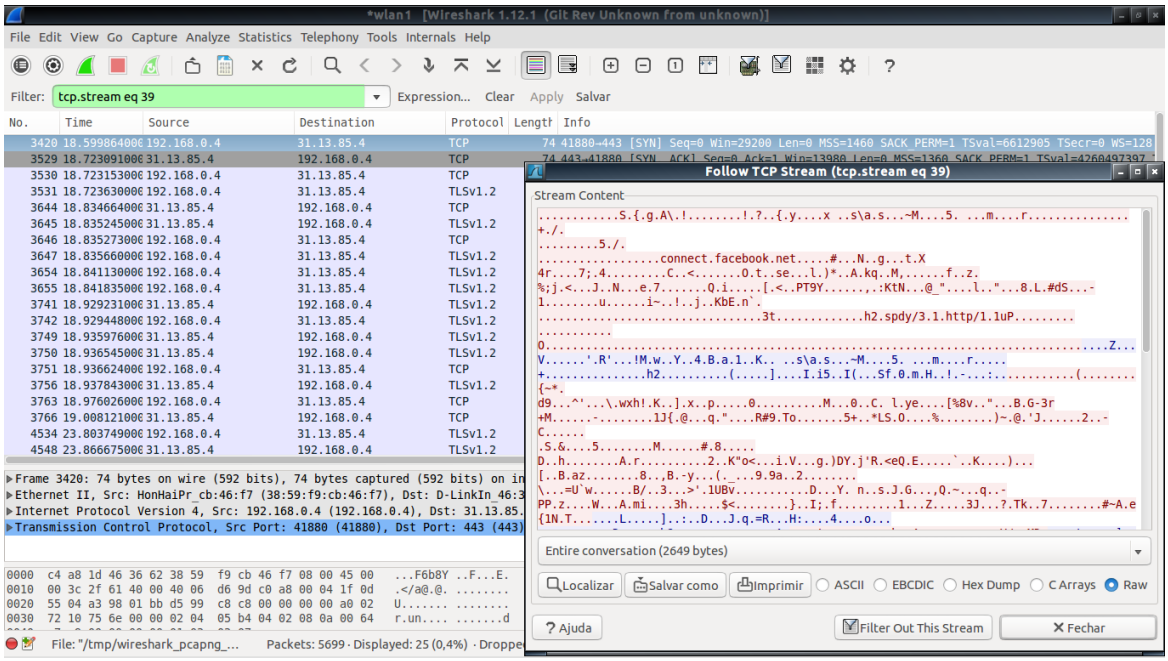
Figura 21 - Pacotes relacionados ao *Facebook*



Fonte: Autoria própria

Escolhemos um pacote TCP SYN/ACK porque este tipo indica que houve uma solicitação de conexão com algum servidor *web* e clicando com o botão direito em cima do pacote e em seguida na opção *follow* TCP *stream* (figura 21), ação para qual conseguimos verificar que a solicitação de conexão foi para *connect.facebook.net* (figura 22).

Figura 22 - Conteúdo de um pacote TCP SYN/ACK



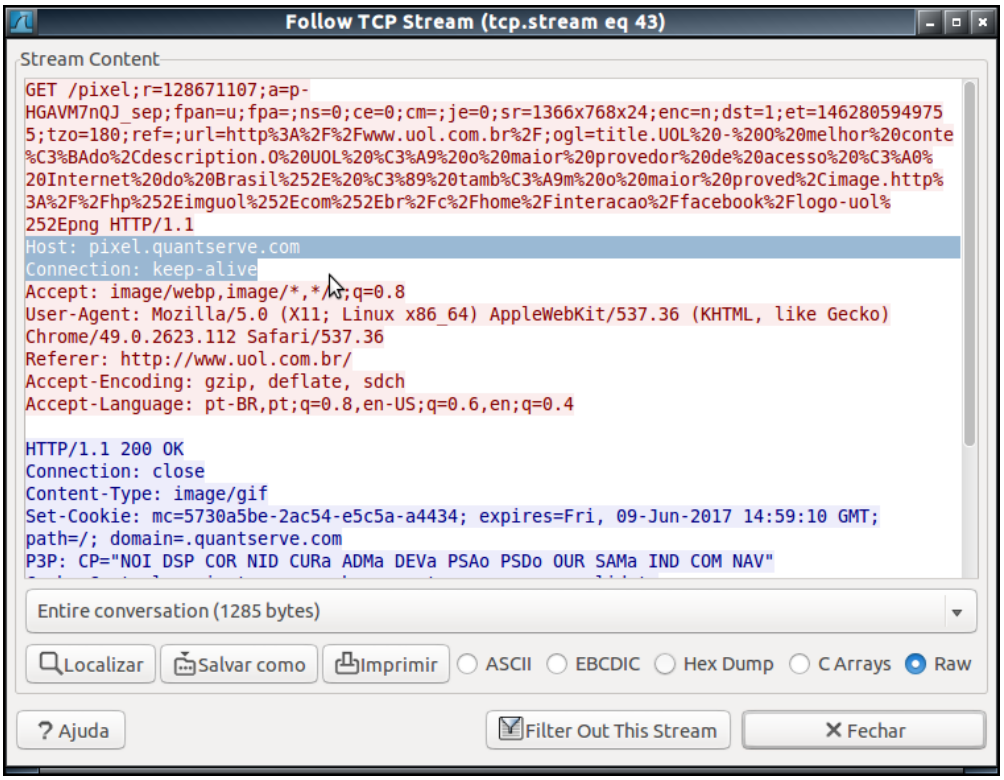
Fonte: Autoria própria.

Porém como visto no histórico, não solicitamos acesso ao portal do Facebook, a provável causa desta solicitação podem ser os *plug-ins* sociais contidos nos *sites* visitados, *pixel tags* ou *cookies* de terceiros, o que não é incomum, visto que não utilizamos navegação anônima e os *cookies* não foram desabilitados.

Ao executar, por exemplo, uma consulta no filtro de pacotes do Wireshark desse modo "*frame contains facebook"*, obtivemos vários resultados contendo pacotes *GET/pixel,* que indicam que um *pixel* foi armazenado na máquina, examinando um destes pacotes, foi possível identificar informações como, por exemplo, a empresa proprietária do *cookie*, o tipo de arquivo e de qual portal partiu esta solicitação.

Devido ao acesso ao site *uol.com.br* este *pixel* foi acionado enviando *cookies* para *pixel.quantserve.com*, o servidor de uma empresa de propaganda baseada em interesse que coleta de informações comportamentais dos usuários.

Figura 23 - *Pixel tag* da empresa Quantserve



Fonte: Autoria própria

Na figura 23 temos a captura de um pacote contendo um pixel da empresa Quantserve, durante a análise dos pacotes foram encontrados diversos outros pacotes *GET/pixel,* consequentemente outros *pixels.*

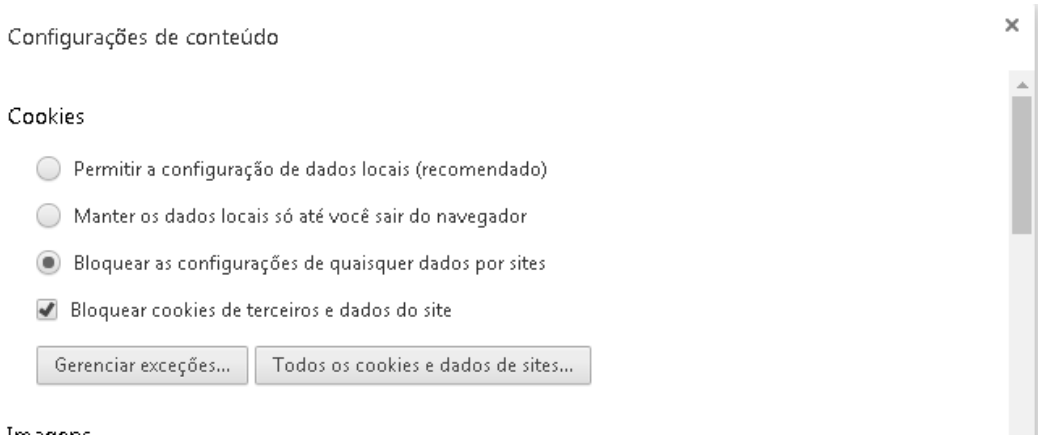
5.3 NAVEGAÇÃO EM MODO ANÔNIMO

Nesta segunda parte do experimento utilizamos as mesmas ferramentas do teste anterior e adicionamos o uso do Sistema Operacional GNU/Linux TAILS, com navegação na Internet pela rede TOR.

Realizamos os testes seguindo alguns procedimentos visando dificultar a coleta dos dados de navegação, o primeiro passo foi desabilitar os *cookie*s nos navegadores;

A figura 24 abaixo mostra o bloqueio de cookies no navegador Google Chrome.

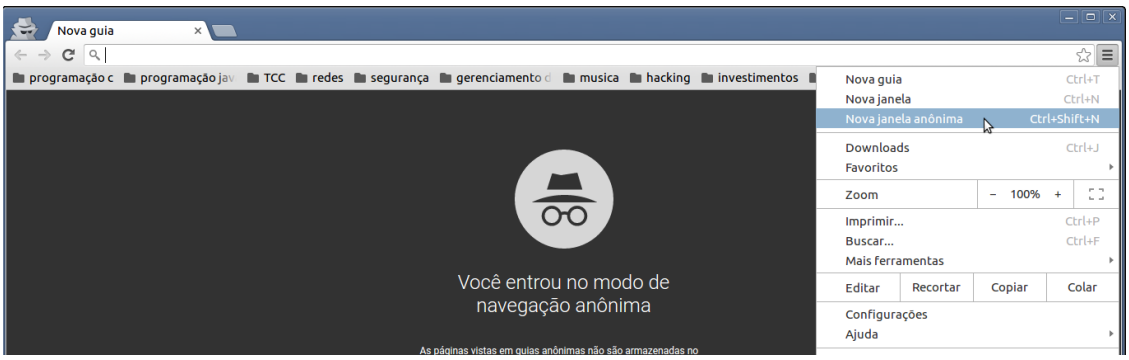
Figura 24 - Bloqueio de *cookies* no navegador



Fonte: Autoria própria

Habilitamos a navegação em modo anônimo;

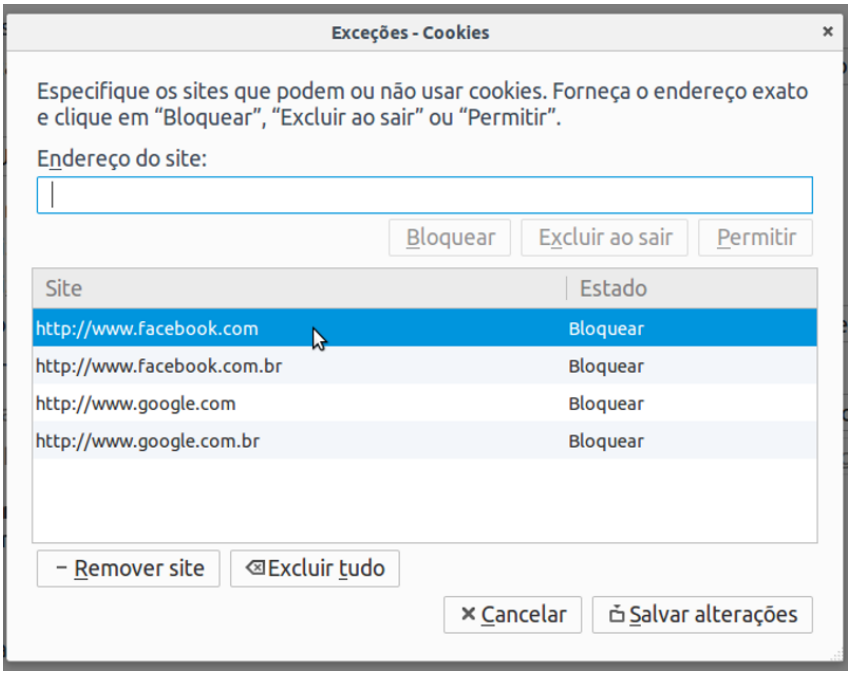
Figura 25 - Navegação em modo anônimo



Fonte: Autoria Própria

Bloqueamos o domínio Facebook.com e Google.com;

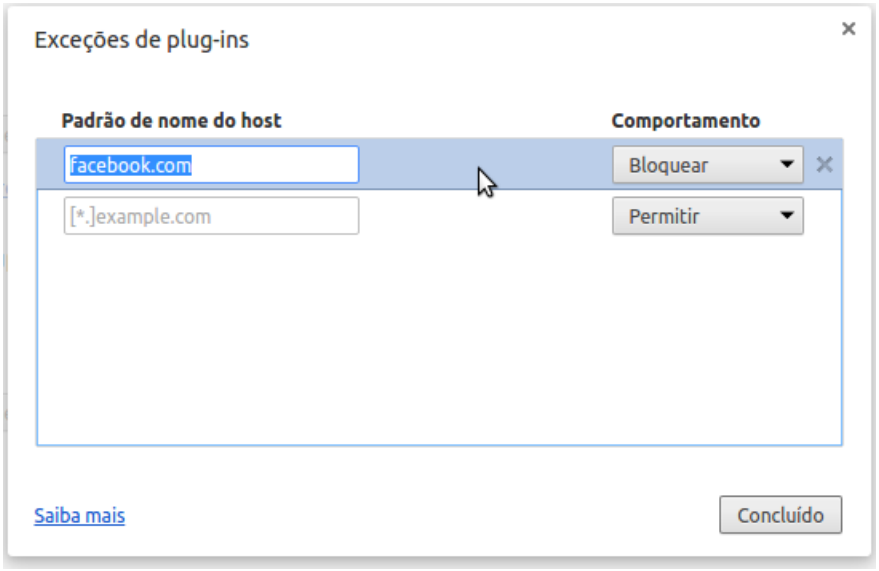
Figura 26 - Sites bloqueados



Fonte: Autoria própria

Logo após realizamos o bloqueio da execução de *plug-ins* pelos navegadores;

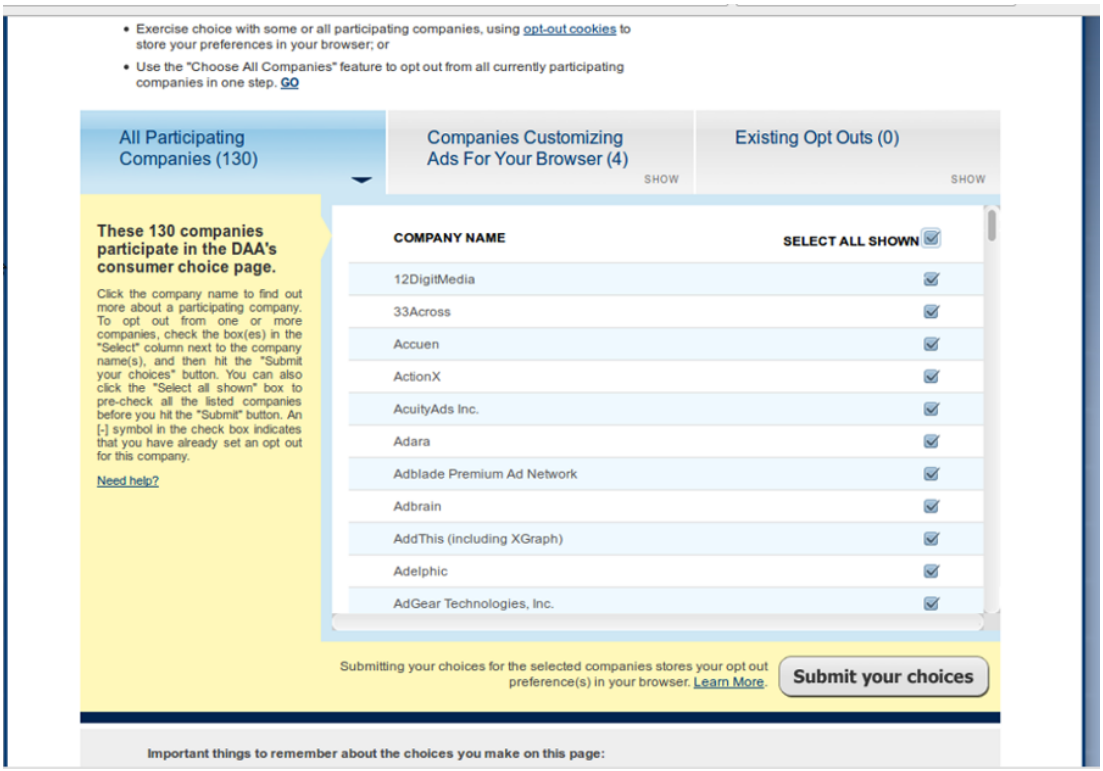
Figura 27 - Bloqueio de *plug-ins*



Fonte: Autoria própria

Em seguida realizamos o *opt-out* junto as entidades nas quais as empresas terceiras, parceiras do *Facebook* que coletam *cookie*s eram ligadas, sendo estas entidades a "*Network Advertising Alliance, Digital Advertising Alliance, European Interactive Digital Advertising Alliance, Digital Advertising Alliance of Canada, Internet Advertising Bureau (US), Internet Advertising Bureau (EU)*" (FACEBOOK, 2016a, p. 4).

Figura 28 - *Opt-out Facebook*



Fonte: Autoria própria

Realizamos o procedimento de *opt-out* também para anunciantes da Google.

Figura 29 - *Opt-out* Google

Fonte: Autoria própria

O próximo passo foi a análise dos pacotes buscando nos filtros do Wireshark pelos IP's e nomes de domínio da Google, Facebook, *cookie*s, *pixel tags* e termos polêmicos, tanto em portais simples como em portais elaborados.

Quadro 1 - Resultado dos testes

Resultados Obtidos						
						Continua
Sites visitados	Ferramentas utilizadas	Modo	Possui Cookies	Possui Pixels	Conexão com Facebook	Conexão com Google
Sites elaborados[1] e termos[2]	Firefox	Normal	Sim	Sim	Sim	Sim
Sites elaborados[1] e termos[2]	Chrome	Normal	Sim	Sim	Sim	Sim
Sites elaborados	Lynx	Anônimo	Não	Não	Não	Não
Sites elaborados[1] e termos[2]	DuckDuckGO	Normal	Sim	Sim	Sim	Sim
Sites elaborados[1] e termos[2]	Tails/Tor	Anônimo	Não	Não	Não	Não
Sites simples[3]	Firefox	Normal	Sim	Não	Não	Não
Sites simples[3]	Chrome	Normal	Sim	Não	Não	Sim
Sites simples[3]	Lynx	Anônimo	Não	Não	Não	Não
Sites simples[3]	DuckDuckGO	Normal	Sim	Não	Não	Não
Sites elaborados[1] e termos[2]	Firefox	Anônimo	Sim	Sim	Sim	Sim
Sites elaborados[1] e termos[2]	Chrome	Anônimo	Sim	Sim	Sim	Sim
Sites elaborados[1] e termos[2]	DuckDuckGO	Anônimo	Sim	Sim	Sim	Sim
Sites simples[3]	Firefox	Anônimo	Sim	Não	Não	Não
Sites simples[3]	Chrome	Anônimo	Sim	Não	Não	Sim
Sites simples[3]	DuckDuckGO	Anônimo	Sim	Não	Não	Não
Sites simples[3]	Tails/Tor	Anônimo	Não	Não	Não	Não

Continuação
1 - Sites elaborados: g1.com.br; uol.com.br; terra.com.br; r7.com.br; bbc.com; globo.com, etc.
2 – Termos: AIDS; Câncer; Homem-bomba; Pedofilia; Atentados; Terrorismo; Obama.
3 – Sites simples[3]: ftp.unicamp.br; gnu.org; pudim.com.br;
Pesquisa realizada entre: 05/05/16 e 01/06/16

Fonte: Autoria própria

Com a análise dos pacotes TCP do *Wireshark* chegamos à conclusão de que as medidas apresentadas como bloqueio de domínios, desativação de *cookie*s, navegação em modo anônimo, *opt-out* ou o buscador DuckDuckGO não impediram que *pixels, cookies* e solicitações de conexão em servidores diferentes dos quais havíamos solicitado ocorressem, as exceções foram as ferramentas Lynx e TOR.

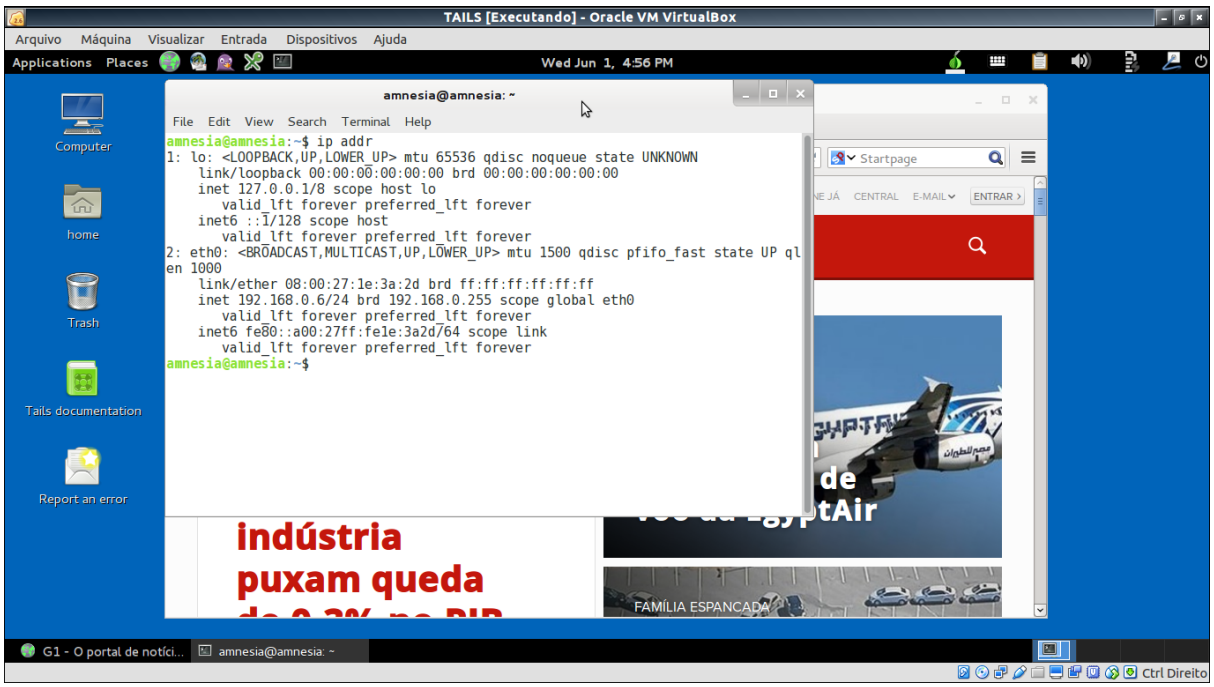
6 CONTRAMEDIDAS CONTRA COLETA INDEVIDA DE DADOS

Com base nos resultados dos testes do capítulo anterior, optou-se por utilizar as ferramentas The Onion Router (TOR) e o The Amnesic Incognito Live System (TAILS), que obtiveram melhor desempenho em relação ao anonimato e privacidade do que as outras ferramentas analisadas.

6.1 TOR e TAILS

Tails é um sistema operacional GNU/Linux baseado no Debian, ele foi projetado para ser usado em DVD, memória USB ou em cartão SD, o objetivo é prover privacidade e anonimato e não deixar rastros do usuário no computador, possui ferramentas no estado da arte em criptografia, e por padrão todas as conexões com a Internet passam obrigatoriamente pela rede TOR, se uma aplicação tentar acessar a Internet diretamente ela é bloqueada por segurança, você pode acessar também a rede I2P, que é uma rede diferente do TOR (TAILS, 2016a).

Figura 30 - Tails no ambiente VirtualBox

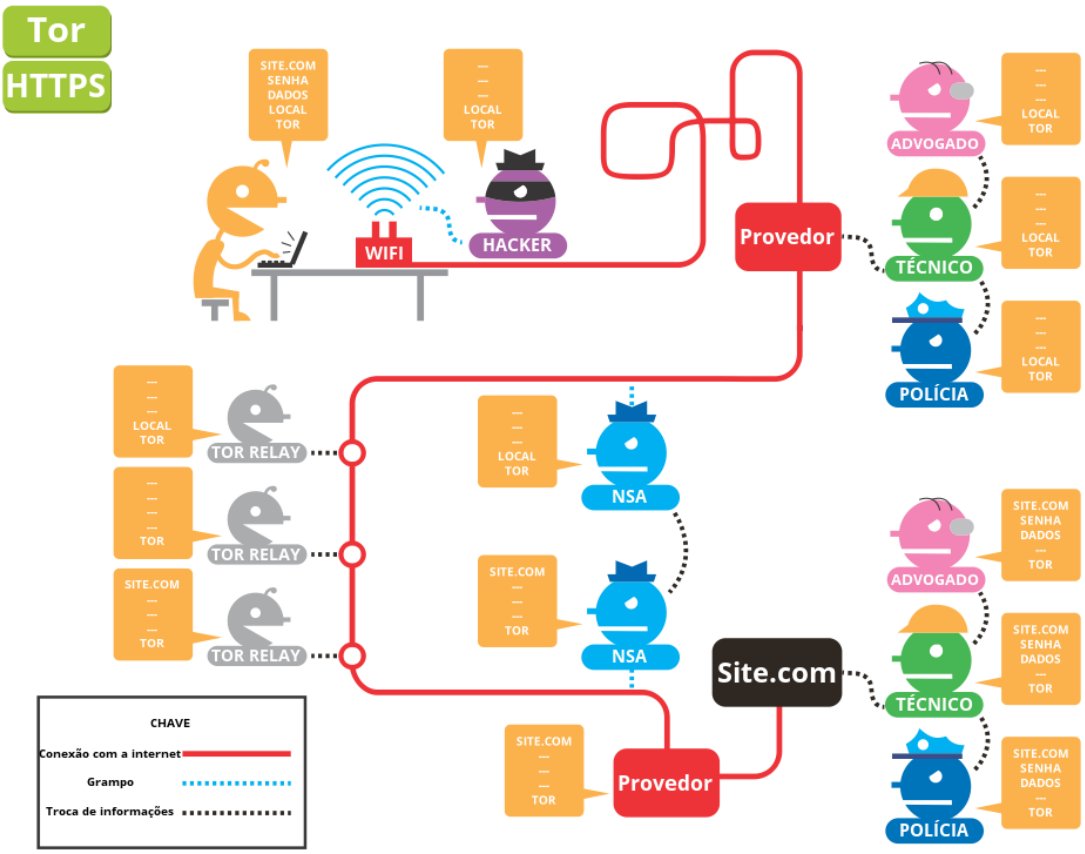


Fonte: Autoria própria

Em nosso teste utilizamos o TAILS em uma máquina virtual conectado em modo Bridge, e desabilitamos o recurso de MAC[12] *spoofing*, que é uma técnica utilizada para mascarar o endereço MAC do adaptador de rede do computador, isto foi necessário para podermos capturar os pacotes no Wireshark, porém como o próprio desenvolvedor esclarece no manual, estas práticas não são recomendadas (TAILS, 2016b).

Mesmo adotando estas medidas os resultados de privacidade e anonimato no TAILS foram satisfatórios.

Figura 31 - Informações visíveis usando TOR



Fonte: OFICINA ANTIVIGILÂNCIA (2015)

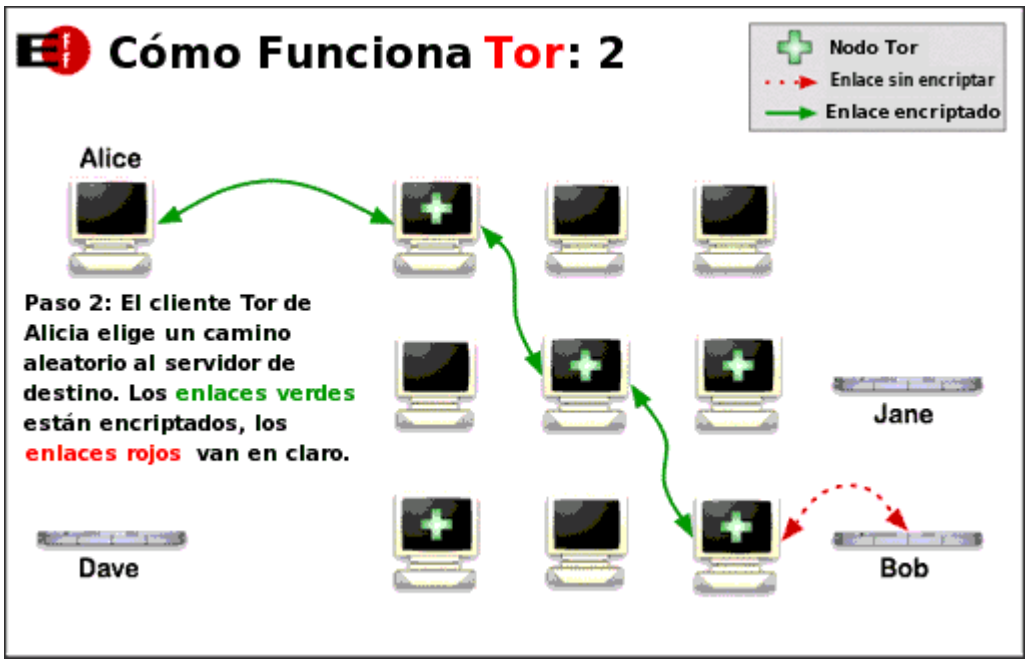
[12] Endereço de interface de rede.

TOR é uma rede de servidores voluntários e anônimos que funcionam como nós da rede, ao utilizar essa rede seu IP é mascarado por uma série de outros IP's espalhados pelo mundo (TOR, 2016).

O único IP que aparece na outra ponta da navegação é o IP do último nó da rede, o que dificulta a descoberta do IP de origem da conexão.

Lembramos aqui que nenhuma ferramenta é capaz de eliminar em 100% os riscos de segurança, o TOR e o TAILS também possuem falhas, e há também problemas relacionados ao ambiente em que os usamos nos quais podem estar comprometidos.

Figura 32 - Rede TOR



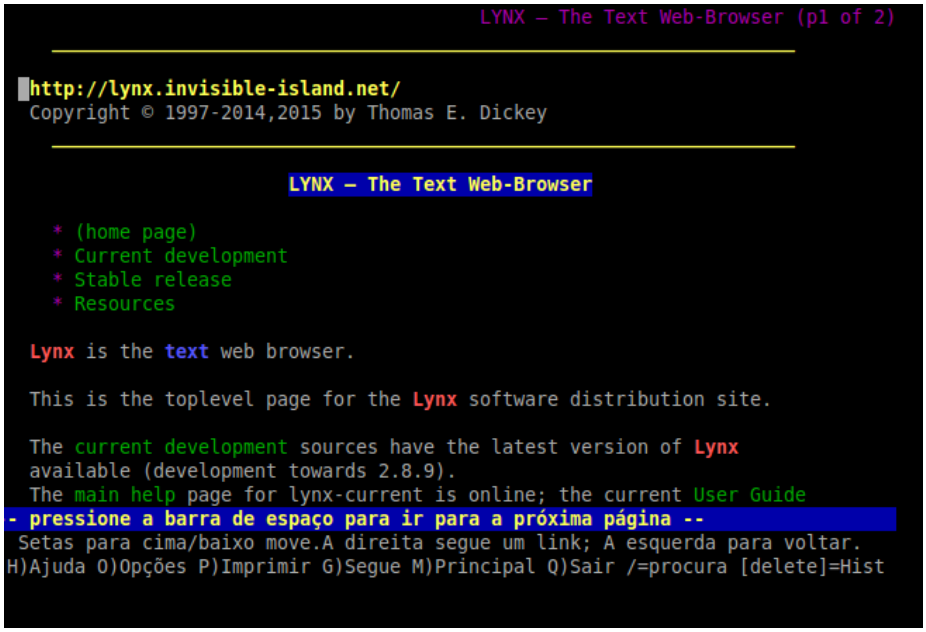
Fonte: OFICINA ANTIVIGILÂNCIA (2015)

Na ilustração da figura 32 podemos observar o funcionamento da rede TOR, a conexão do usuário irá atravessar diversos nós da rede presentes em diferentes localidades, cada nó possui sua localização protegida por criptografia, assim apenas o último nó poderá ser identificado. Se, por exemplo, o usuário estiver no Brasil e quiser se comunicar com alguém no Canadá e o último nó estiver localizado na Rússia, alguém que tentar interceptar a comunicação pensará que o emissor está na Rússia e não no Brasil.

6.2 LYNX

Lynx é um navegador em modo texto para sistemas GNU/Linux que pode ser acessado pelo terminal, possui diversas opções, dentre elas destacamos a de negar todos os *cookies* da página, devido à sua simplicidade e ao fato de não executar *plug-ins* ou baixar imagens acaba por se tornar uma boa opção para quem não quer ter seus dados de navegação compartilhados através de *cookies* e *pixels*.

Figura 33 - Lynx



Fonte: Autoria própria

A figura 33 exibe a tela inicial do navegador em modo texto Lynx, que pode ser executado via linha de comando no Terminal do GNU/Linux.

CONSIDERAÇÕES FINAIS

A cada atividade que todos nós realizamos na grande rede, cada passo, cada opinião ou compra, cada vídeo ou jogo, absolutamente tudo está passível de vigilância como em um pesadelo moderno descrito há quase 70 anos por George Orwell em seu livro “1984”.

A partir da apresentação e análise dos dados, constatou-se a coleta de informações, por vezes sem o consentimento expresso e ciente dos usuários, como exigem as diversas leis nacionais e internacionais e sem as partes coletoras informarem de maneira clara e objetiva os propósitos da coleta, se há ou não condições de assegurar a confidencialidade destas informações e seu uso idôneo por parte de empresas e/ou governos.

Vimos também que agências de inteligência, órgãos governamentais e empresas estão envolvidos em casos de coleta e uso indevido de informações, entrando no campo ético-moral em que questionamos se os fins, como a segurança nacional ou a obtenção de maiores lucros justificam, por exemplo, os meios utilizados para tal.

Vimos, por exemplo, no experimento prático que é possível saber quem coleta e o que está sendo coletado quando acessamos a Internet.

Atrelado às questões supracitadas, pode-se em hipoteticamente afirmar que o risco de ser monitorado mesmo utilizando ferramentas como desativação de *cookies*, navegação anônima, *opt-out*, ou até mesmo o uso de redes anônimas e criptografadas, como o TOR o qual podem prometer anonimato, não podem ser eliminados, mas sim mitigados, pois todos os dias novas vulnerabilidades são descobertas e exploradas.

Este trabalho deixa aberta para obras futuras sobre a temática a possibilidade de uma investigação e a proposição de contramedidas mais profundas.

REFERÊNCIAS

ALLAN, Alasdair; WARDEN, Pete. ***Got an* iPhone *o* 3G iPad*?* Apple *is recording your moves****.*** *A hidden file in* iOS 4 *is regularly recording the position of devices.* 20 abr. 2011. Disponível em: <http://radar.oreilly.com/2011/04/apple-location-tracking.html>. Acesso em: 15 maio. 2016.

ALPEROVITCH, Dmitri. ***Revelead*:** *Operation* Shady RAT. 2011. Disponível em: <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>. Acesso em: 22 mar. 2016.

ALSENOY. Brendan V. *et al.* ***From social media service to advertising network:*** *A critical analysis of Facebook's Revised Policies and Terms.* 25 ago. 2015. Disponível em: <https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf>. Acesso em: 07 abr. 2016.

ANISTIA INTERNACIONAL. **Opinião pública:** vigilância e privacidade na internet. 18 mar. 2015. Estudo conduzido pelo YouGov. Disponível em: <https://anistia.org.br/wp-content/uploads/2015/03/Dados-vigil%C3%A2ncia-e-privacidade_Anistia-Internacional1.pdf >. Acesso em: 22 mar. 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da Informação:** Técnicas de segurança: Código de práticas para controles de segurança da informação: NBR ISO/IEC 27002. Rio de Janeiro, 2013.

_____. **Tecnologia da Informação:** Técnicas de segurança: Sistemas de gestão de segurança da informação: Requisitos: NBR ISO/IEC 27001. Rio de Janeiro, 2013.

BARTH. Adam. **RFC 6265:** HTTP *State Management Mechanism*. Berkeley. 2011. Disponível em: <https://tools.itef.org/html/rfc6265>. Acesso em: 28 jun. 2016.

BÉLGICA. Comission Nationale de L'informatique et des Libertés. **Google pryvacy policy:** Main findings and recommendations. Bruxelas. 2012. Apêndice do artigo WP29. Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf>. Acesso em: 24 mar. 2016.

BÉLGICA. *The Commision for protection of privacy*. ***Recommendation* nº 04/2015 of 13 *May* 2015**. Bruxelas. 2015. Disponível em: <https://www.privacycommission.be/sites/privacycommission/files/documents/recommendation_04_2015_0.pdf>. Acesso em: 22 mar. 2016.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Política de privacidade.** [S.l.], v. 0.2, p. 2, 08 abr. 2015. Disponível em: <www.cgi.br/politica-de-privacidade/>. Acesso em: 15 maio. 2016.

_____. **Resolução CGI.br/RES/2013/020**, de 2013. Posicionamento do CGI.br sobre coleta de dados de usuários finais na Internet pela *National Security Agency (*NSA*)* dos EUA. Resoluções**,** São Paulo, SP, p. 1, jul. 2013. Disponível em: <http://www.cgi.br/resolucoes/documento/2013/020>. Acesso em: 22 mar. 2016.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, 5 de outubro de 1988. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/legislacao/Constituicoes_Brasileiras/constituicao1988.html>. Acesso em: 28 de maio de 2015.

_____. **Lei n. 12.965, de 23 de abril de 2014.** Marco Civil da Internet. Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 mar de 2016.

BRIGHT, Peter. ***Even when told not to,* Windows 10 *just can´t stop talking to* Microsoft:** *It's no wonder that privacy activists are up in arms.* 13 ago. 2015. Disponível em:<http://arstechnica.co.uk/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/>. Acesso em: 30 maio. 2016.

CALIFÓRNIA(USA). *California Northern District Court*. *Oakland Office*. **Processo n. 5:2013cv05996**. Outras Ações Legais. Reclamantes: Matthew Campbell e Michael Hurley. Acusada: Facebook, Inc. Califórnia 30 de dezembro de 2013.Disponível em: <https://dockets.justia.com/docket/california/candce/5:2013cv05996/273216>. Acesso em: 08 abr. 2016.

_____. *California Northern District Court*. *San Jose Office*. **Processo n.5:2010cv03272**. Outras Injúrias Pessoais. Reclamantes: Jennifer Locsin e James Blackwell. Acusada: Google, Inc. Califórnia 26 de julho de 2010.Disponível em: <https://dockets.justia.com/docket/california/candce/5:2010cv03272/230000>. Acesso em: 08 abr. 2016.

CORÉIA do Sul é o 1º país a multar Apple por coleta indevida de dados dos usuários de iPhone. **O Globo** 03 ago. 2011. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/coreia-do-sul-o-1-pais-multar-apple-por-coleta-indevida-de-dados-dos-usuarios-de-iphone-2871131>. Acesso em: 12 maio. 2016.

FACEBOOK. **Cookies, Pixels e Tecnologias similares**. 2016. Disponível em: <https://www.facebook.com/policy/cookies>. Acesso em: 11 maio. 2016.

FACEBOOK. **Exemplo de código completo**. 2016. Disponível em: Disponível em: <https://developers.facebook.com/docs/plugins/like-button#example>. Acesso em: 15 maio. 2016.

FACEBOOK. **Facebook pixel base code**. 2016. Disponível em: <https://pt-br.facebook.com/business/help/952192354843755>. Acesso em: 15 maio. 2016.

FINKLE, Jim. **Descoberta a maior série de ataques *hackers* da história**. Reuters. Boston, 03 ago. 2011. Disponível em: <http://br.reuters.com/article/idBRSPE77208020110803>. Acesso em: 22 mar. 2016.

FOULCAULT, Michel. **Vigiar e punir:** Nascimento da prisão. 29. ed. Tradução de Raquel Ramalhete. Petrópolis: Vozes, 2004. p. 262.

GALLAGHER, Ryan. ***British spy chiefs secretly begged to play in NSA's data pools***. The Intercept. [S.l.]. 30 abr. 2014. Disponível em:< https://theintercept.com/2014/04/30/gchq-prism-nsa-fisa-unsupervised-access-snowden/>. Acesso em: 31 mar. 2016.

GALLI, Marcelo. **Bisbilhoteiros virtuais:** Empresa italiana de vigilância digital é contratada por governos é hackeada. 23 jul. 2015. Disponível em: <http://www.conjur.com.br/2015-jul-23/empresa-vigilancia-digital-usada-governos-hackeada>. Acesso em: 08 abr. 2016.

GEARY, Joanna. ***Tracking the trackers:*** *What are cookie? An introduction to web tracking*. The Guardian, Londres, 15 out. 2012. Disponível em: https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro>. Acesso em: 25 abr. 2016

GRUPO GLOBO. **Política de privacidade Globo.com**. 2015. Disponível em: <www.globo.com/privacidade.html>. Acesso em: 15 maio. 2016.

GOOGLE. **A *simple* *button***. 2015. Disponível em:<https://developers.google.com/+/web/+1button/#getting-started>. Acesso em 15 maio. 2016.

GREENWALD, Glenn. **Sem lugar para se esconder.** Tradução de Fernanda Abreu. Rio de Janeiro: Sextante, 2014. 269 p.

_____ . **XKeyscore:** NSA t*ool collects 'nearly everthing a user does on the internet'*. Londres, 31 jul. 2013. Disponível em: <https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>. Acesso em: 31 mar. 2016.

HENRIQUES. M. S. B. *et al.* **BIG DATA.** Revista Pensar Tecnologia. [S. l.]. vol. 2, n. 2, jul. 2013. Disponível em: <revistapensar.com.br/tecnologia/pasta_upload/artigos/a55.pdf>. Acesso em: 28 jun. 2016.

IRLANDA. Supremo Tribunal de Justiça (High Court of Ireland). Acórdão. Reenvio prejudicial – Dados pessoais – Proteção das pessoas singulares no que diz respeito ao tratamento desses dados – Carta dos Direitos Fundamentais da União Europeia – Artigos 7.°, 8.° e 47.° – Diretiva 95/46/CE – Artigos 25.° e 28.° – Transferência de dados pessoais para países terceiros – Decisão 2000/520/CE – Transferência de dados pessoais para os Estados Unidos – Nível de proteção inadequado – Validade – Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos – Poderes das autoridades nacionais de controlo. Pedido de decisão prejudicial. Processo C-362/14. Recorrente: MaximillianSchrems. Recorrido: Data Protection Commissioner. Relator: T. Von Danwitz. Dublin, 06 out. 2015. **InfoCuria – Jurisprudência do Tribunal de Justiça,** Dublin, out. 2015. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?docid=169195&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=PT&cid=227891 >. Acesso em: 29 maio. 2016.

KUROSE. James F; ROSS. Keith W. **Redes de Computadores e a Internet:** uma abordagem *top-down*. Tradução: Opportunity Translations. 5ª. ed. São Paulo: Pearson, 2010. 592 p.

MACASKILL, Ewen *et al.* **GCHQ *taps fibre-optic cables for secret access to world's communications.*** The Guardian, Londres, 21 jun. 2013. Disponível em: <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>. Acesso em: 24 mar. 2016.

MICROSOFT. **Política de privacidade da Microsoft**. 2016. Disponível em: <https://privacy.microsoft.com/pt-br/privacystatement>. Acesso em: 12 maio. 2016.

NSA *Slides explain the* PRISM *data-collection program*. **The Washington Post**. [S.l.], 6 jun. 2013. Disponível em: <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. Acesso em: 31 mar. 2016.

OFICINA ANTIVIGILÂNCIA. **TOR e HTTPS**. Disponível em: <https://antivigilancia.org/pt/tor-e-https/ >. Acesso em: 02 jun. 2016.

PORTAL TERRA. **Privacidade**. 2016. Disponível em: <www.terra.com.br/avisolegal/privacidade.html>. Acesso em: 15 maio. 2016.

PORTAL UOL. **Normas de segurança e privacidade**. 2016. Disponível em: <https://sac.uol.com.br/#/wrapper?url=https:%2F%2Fsac.uol.com.br%2Finfo%2Fprotecao_privacidade%2Fnormas_protecao_privacidade.jhtm>. Acesso em: 15 maio. 2016.

RAYMOND. Erick S. **Como se tornar um *hacker.*** Tradução: Rafael Caetano dos Santos. 05 jun. 1998. Disponível em: <https://www.linux.ime.usp.br/~rcaetano/docs/hacker-howto-pt.html>. Acesso em: 27 jun. 2016.

RUBIN, Julia *et al*. Massachusetts Institute of Technology, USA, Global InfoTek, Inc, USA. ***Convert communication in mobile applications***. 2015. 30th IEEE/ACM International Conference on Automated Software Engineering (ASE). Disponível em: <https://people.csail.mit.edu/mjulia/publications/Covert_Communication_in_Mobile_Applications_2015.pdf>. Acesso em: 22 mar. 2016.

SIGNAL. **Tag Management 101**, 2010-2016. Disponível em: <www.signal.co/resources/tag-management-101 >. Acesso em: 15 maio. 2016.

THE AMNESIC INCOGNITO LIVE SYSTEM (TAILS). **Sobre**. 2016. Disponível em: <https://tails.boum.org/about/index.pt.html>. Acesso em: 15 maio. 2016.

_____. ***Virtualization***. 2016. Disponível em: <https://tails.boum.org/doc/advanced_topics/virtualization/index.en.html#security>. Acesso em 15 maio. 2016.

TANENBAUM. Andrew S. **Redes de computadores.** Trad. Vandenberg D. Souza. 4ª. ed. Rio de Janeiro: Campus, 2003. 632 p.

THE ONION ROUTER. **Tor:** Overview. 2016. Disponível em: <https://www.torproject.org/about/overview.html.en>. Acesso em 14 maio. 2016.

TORRES, Gabriel. **Redes de computadores curso completo**. Rio de Janeiro: Axcel Books do Brasil, 2001. 664 p.

TWITTER. ***How to add a tweet button to your web site***. 2016. Disponível em: <https://dev.twitter.com/web/tweet-button>. Acesso em: 15 maio. 2016.

THE MOSCOW TIMES. **Moscow *lawyers complain to prosecutors over* Windows 10 *privacy*.** 20 ago. 2015. Disponível em: <http://www.themoscowtimes.com/news/article/moscow-lawyers-complain-to-prosecutors-over-windows-10-privacy/528310.html>. Acesso em: 30 maio. 2016.