Universidade Católica de Brasília

Pró-Reitoria Acadêmica
Escola Politécnica
Trabalho de Conclusão de Curso

ANÁLISE E IDENTIFICAÇÃO DE AUTORIA DE E-MAIL

Autor: Givailson de Souza Neves
Orientador: Esp. João Eriberto Mota Filho

Brasília - DF
2015

GIVAILSON DE SOUZA NEVES

ANÁLISE E IDENTIFICAÇÃO DE AUTORIA DE E-MAIL

Artigo apresentado ao Programa de Pós-Graduação Stricto Sensu em Perícia Digital da Universidade Católica de Brasília, como requisito parcial para obtenção do Título de Especialista em Perícia Digital.

Orientador: Esp. João Eriberto Mota Filho

Brasília
2015

Artigo de autoria de Erivelto Drumond Ponte, intitulado "MARCO CIVIL DA INTERNET VERSUS PERÍCIA DIGITAL", apresentado como requisito parcial para obtenção do diploma de conclusão de curso de especialização em Perícia Digital da Universidade Católica de Brasília, em _____de _____de 2015, defendido e aprovado, pela banca examinadora abaixo assinada:

_____

Professor Esp. João Eriberto Mota Filho
Orientador
Curso de Perícia Digital - UCB

_____

Professor Esp. Alexandre Antonio Antunes Almeida
Examinador
Curso de Perícia Digital - UCB

Brasília
2015

Dedico este trabalho aos meus pais – João de Souza Neves e Creonilta de Jesus Souza Neves – que, mesmo nos momentos difíceis, sempre fizeram o possível para garantir a minha educação e a do meu irmão.

AGRADECIMENTOS

A todos os meus professores, que nos elogios ou nas críticas, não deixaram de me incentivar ao longo de minha jornada até aqui. Aos meus colegas de sala, Pedro e Magno, por sempre me apoiarem e auxiliarem nos trabalhos dentro e fora de sala.

ANÁLISE E IDENTIFICAÇÃO DE AUTORIA DE E-MAIL

GIVAILSON DE SOUZA NEVES

Resumo:
Muitas são as ameaças que circundam os usuários de e-mail nos tempos atuais. Captura de dados e instalações de softwares maliciosos são apenas alguns dos exemplos onde podem ocorrer ataques diretos aos usuários. Isso sem falar dos criminosos que utilizam o e-mail como forma de disseminar conteúdo ilícito, como é o caso dos pedófilos. Este Artigo Técnico detalhou o processo de envio e recebimento de um e-mail e como o conhecimento da formação básica de seu cabeçalho é importante para um perito forense. Para a realização deste estudo empírico foi realizada uma pesquisa exploratória, tendo por base, pesquisa aplicada, bibliográfica e estudo de caso sobre a história do e-mail, sua composição e os meios com os quais um perito normalmente conta para a localização do remetente. Após um estudo de caso envolvendo o cabeçalho de dois e-mails, enviados um de forma padrão e outro de forma anônima, foi possível verificar a localização da autoria e os passos necessários para a identificação do remetente.

Palavras-chave: E-mail. Perícia forense. Fraudes eletrônicas.

1 INTRODUÇÃO

O e-mail talvez seja a forma de comunicação mais antiga disponível na computação. Em um primeiro momento o ele era, apenas, uma forma de comunicação entre usuários de um *mainframe.* Tantas são as possibilidades que ao certo não é possível precisar qual tecnologia foi utilizada nas primeiras trocas de mensagem eletrônicas.

Após o surgimento da primeira rede de computadores, *ARPANET*, o e-mail, como é conhecido hoje, começou a ganhar forma. Computadores separados por quilômetros de distância agora permitiriam que seus usuários interagissem por meio de mensagens de texto.

Em meados dos anos 60, o e-mail se popularizou rapidamente como forma de comunicação e mesmo nos dias de hoje com o advento das mensagens instantâneas, videoconferências, redes sociais etc., ele ainda é uma ferramenta extremante útil.

Um dos fatores cruciais para a aceitação e uso massificado do e-mail, foi a aposta de várias empresas nesta tecnologia. Empresas como o POP chegaram a, além de fornecerem o serviço de provedor de internet, disponibilizar contas gratuitas de e-mail. Até nos dias de hoje muitas são as empresas que oferecem esse serviço, e entre essas podemos destacar o Google, a Microsoft e o Yahoo, que além da gratuidade do serviço disponibilizam espaço quase ilimitado de armazenamento.

Atualmente, o e-mail é utilizado para vários assuntos, dentre os quais podemos destacar: como ferramenta de trabalho, para fins acadêmicos e até para envio e recebimento de arquivos, que neste caso podem ser, inclusive, documentos pessoais e faturas de serviços. O e-mail tem se tornado cada vez mais uma

ferramenta formal de troca de conteúdos, talvez por isso os criminosos digitais tenham dado tanta atenção a ele como forma de obter vantagens ilícitas.

As técnicas e estratégias têm evoluído tanto que cada vez mais os e-mails e as comunicações digitais vêm merecendo uma maior atenção dos profissionais de segurança da informação. Segundo o último relatório de segurança disponibilizado pela Symatec, com dados de 2014, muitos dos ataques a usuários de e-mail são na modalidade de *Phishing* e *Spear-phishing.* Entre os artifícios utilizados para obter lucro por meio de fraudes está a instalação de softwares maliciosos, pois contando principalmente com recursos de engenharia social, os criminosos tentam ludibriar os usuários induzindo-os a instalar os *s*oftwares ou ainda fornecer dados pessoais sobre falsos pretextos.

Com pouco conhecimento em programação ou desenvolvimento de *websites* é possível fazer uma réplica fiel, ou ainda que inspire confiança, de e-mails e sites de instituições sérias como bancos e órgãos públicos. A artimanha é tanta que na maioria dos casos a fraude é deflagrada para públicos específicos ou ainda em épocas que facilitem a indução ao engano, tornando as vítimas mais suscetíveis ao golpe.

No Brasil, é muito comum na época de declaração de imposto de renda o recebimento de e-mails, ditos serem de autoria da Receita Federal Brasileira, que solicitam ao usuário dados pessoais ou ainda os encaminham a sites feitos com o único propósito de capturar informações. E apesar da massiva campanha que ocorrem em jornais e sites oficiais, ainda são muitos os casos de pessoas fraudadas.

Não podemos deixar de mencionar que o e-mail também é uma forma de trocar conteúdos grandes, como arquivos compactados, fotos e até vídeos e, infelizmente, dentre o conteúdo trafegado existem aqueles que são de natureza ilícita. Destes, talvez um dos mais preocupantes e que merece uma atenção diferenciada é o de pornografia infantil. A pedofilia é um dos crimes que mais utiliza o e-mail como uma de suas principais formas de disseminação. Para a troca de material ilícito o usuário, com o intuito de ocultar-se, pode fazer uso de ferramentas de criação de e-mails anônimos ou ainda utilizar servidores que realizam este serviço. Forjar um e-mail não é uma tarefa que necessite grandes conhecimentos em informática, uma rápida busca na internet e vários serão os resultados que prometem e que fazem esse serviço. Contudo, quão anônimos são realmente esses e-mails? Será de fato possível ocultar todos os vestígios que identifiquem a origem e a autoria da mensagem?

Com tantas fraudes e materiais ilícitos circulando pela internet, quais são as técnicas e conhecimentos que um perito forense conta para elucidar investigações? Como está previsto na legislação brasileira sobre a quebra de sigilo destas informações? São estas as questões que ao longo deste trabalho serão abordadas, além de descrever o funcionamento do e-mail e os procedimentos necessários à identificação do responsável.

1.1 JUSTIFICATIVA

Muitas são as ameaças que circundam os usuários de e-mail nos tempos atuais. Captura de dados e instalações de softwares maliciosos são apenas alguns dos exemplos dos perigos que cercam os usuários deste tipo de aplicação. Isso sem falar dos criminosos que descobriam no e-mail uma forma de disseminar conteúdo ilícito, como é o caso dos pedófilos. Neste projeto tem por objetivo principal o

esclarecimento dos processos envolvidos na identificação da origem e autoria de e-mails enviados por meio comum e anônimo. Não serão aqui contempladas as mensagens enviadas por ferramentas de ocultação de autoria.

1.2 CONTEXTUALIZAÇÃO DO PROBLEMA E O PROBLEMA

Como analisar a origem e a autoria de um e-mail? Quais os artifícios e técnicas podem ser utilizadas por um perito em forense computacional neste processo?

1.3 PRESSUPOSTO DA PESQUISA

Através da análise do processo de criação, composição e envio de um e-mail. Pretende-se identificar os elementos responsáveis pelo envio e entrega de uma mensagem de correio eletrônico e com base nestas informações localizar sua origem e responsável.

1.4 PROPÓSITO

O conhecimento da historia e do funcionamento de um e-mail não é de conhecimento geral. Mesmos os profissionais de informática não possuem uma correta noção sobre a composição de uma mensagem, e dos processos envolvidos no seu envio e recebimento.

Tendo em vista a crescente necessidade do conhecimento de como é o processo de localizar o responsável e a origem de um e-mail. Este artigo tem o objetivo a seguir:

1.4.1 Objetivo Geral

Demonstrar os passos necessários para a realização do processo de identificação de autoria e origem de um e-mail.

1.4.2 Objetivos Específicos

Para alcançar o objetivo geral foi necessário:

a) Explicar como se realiza o processo de envio e recebimento de um e-mail, desde a criação do e-mail até a recepção por parte do destinatário;
b) Identificar as formas mais comuns de ameaça e os fins ilícitos para os quais um e-mail pode ser utilizado; e
c) Demonstrar os passos necessários para a identificação da origem e autoria de um e-mail;

1.5 ORGANIZAÇÃO DO TRABALHO

Este trabalho está dividido da seguinte maneira:

a) Introdução que faz uma breve explanação sobre a importância do e-mail, seus principais usos e ameaças;
b) Referencial Teórico que busca embasar a pesquisa com conceitos e definições de autores de renome, fornecendo os insumos necessários para a correta compreensão do tema;

c) A terceira parte delineia as Metodologias de Pesquisa, bem como os procedimentos a serem realizados no estudo de caso apresentado; e
d) A parte final demonstra os resultados obtidos no estudo de caso, incluindo demais explicações necessárias ao entendimento dos processos que se deverão seguir. Ao que se resulta nas conclusões e opiniões do autor sobre o tema estudado.

2 REFERENCIAL TEÓRICO

A seguir serão apresentados conceitos sobre mensagens eletrônicas, sua origem e sua importância como meio de comunicação individual e coletiva. Serão relacionadas, também, as tecnologias envolvidas no processo de envio e recebimento de uma mensagem eletrônica, bem como as fraudes que podem ser realizadas por este meio, incluindo os processos mais comumente utilizados na identificação da autoria de um e-mail.

2.1 A HISTÓRIA DO E-MAIL

A comunicação por meio de mensagens eletrônicas não é algo novo, já está presente desde os primórdios da computação. Conforme cita Antônio Lemos Sampaio (2011), as mensagens eletrônicas sugiram em meados da década de 60 como uma forma de comunicação entre usuários de *mainframes, s*endo, inclusive, difícil precisar qual sistema de correio eletrônico deu início a esta tecnologia. Já em 1971 o símbolo @ (*at*), conhecido no Brasil como arroba, foi introduzido nas comunicações com o propósito de indicar o domínio ao qual pertence o usuário. Assim, por exemplo, “joão@ucb” indicaria “João da UCB”.

Após um breve período de expansão das redes de computadores, culminando na hoje conhecida *internet,* surgiram várias empresas que se especializaram em fornecer serviços de correio eletrônico e a maioria de forma gratuita. Entre os e-mails gratuitos mais comumente utilizados, podemos destacar o *Hotmail*, o *Yahoo*, e o *Gmail*. A disponibilização de serviços gratuitos e a facilidade de criar um e-mail, que muitas vezes consiste apenas no preenchimento de um formulário, ajudou muito a disseminar o seu uso como uma forma não somente de comunicação pessoal, mas também uma ferramenta de trabalho. Sua popularidade cresceu tanto que o e-mail já vem sendo aceito como prova documental em ações judiciais. E, consequentemente, com o uso em larga escala dos e-mails como forma de comunicação, vulnerabilidades foram encontradas e logo surgiram as fraudes. Tudo isso devido à facilidade em criar uma conta válida mesmo que com dados falsos, facilitando o acesso para que um indivíduo com propósitos ilícitos possa deflagrar ataques maliciosos que visam tanto o dano direto, quanto a invasão de sistemas de informação.

2.2 O FUNCIONAMENTO DE UM E-MAIL

Um sistema de correio eletrônico é composto por programas de computador que são responsáveis pelo envio da mensagem de um cliente para um servidor. Segundo Goodrich, Michael T. e Tamassia, Roberto (2013) o processo de envio de uma mensagem SMTP (Simple Mail Transfer Protocol) é feita quando o cliente de um e-mail que é conhecido com *Mail User Agent* (MUA) envia uma mensagem SMTP para um *Mail Sending Agent* (MSA), que por sua vez despacha a mensagem

para um *Mail Transfer Agent* (MTA) responsável por enviar a mensagem ao destinatário.

Um e-mail, segundo a IETF (RFC 5322), é composto por basicamente duas seções principais:

- Cabeçalho – é composto por linhas que contém o nome do campo e o valor do campo, separados pelo símbolo de dois pontos (:). O nome do campo deve conter de 33 a 126 caracteres imprimíveis no formato US-ASCII. Já o conteúdo deve ser composto de caracteres US-ASCII e pode conter espaços em branco e tabulações.
- Corpo – é a mensagem na íntegra que consiste de uma sequência de caracteres em formato US-ASCII.

A constituição de um e-mail é relativamente simples, porém existem regras de formatação que são definidos principalmente pela RFC 5322 de 2008. As RFCs (*Request for Comments*) por sua vez são criadas e mantidas pela IETF (*Internet Engineering Task Force*), que consiste de um grupo de trabalho internacional cuja principal função é criar padrões para a internet por meio das RFC.

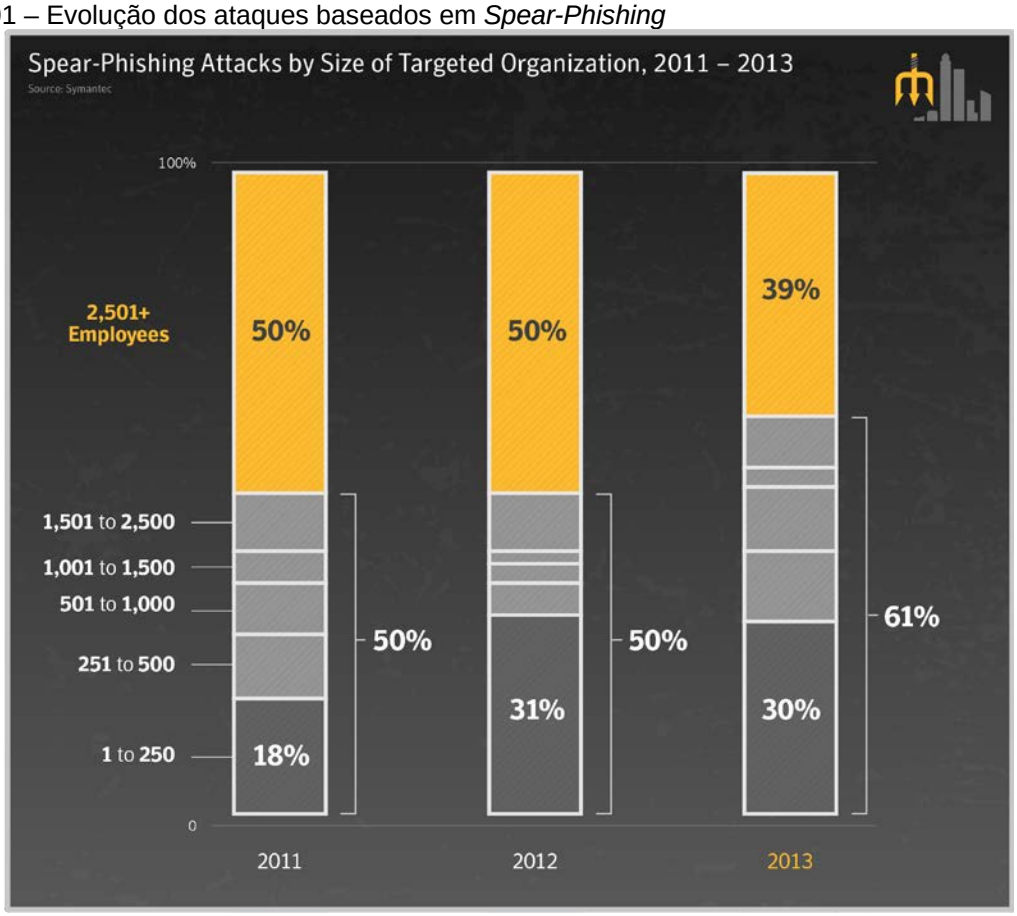
2.3 CRIMES E FRAUDES POR E-MAIL

Com a popularização do uso do e-mail como ferramenta de comunicação, este passou também a ser utilizado como uma ferramenta para crimes ou desavenças pessoais. Eleutério, Pedro Monteiro da Silva e Machado, Márcio Pereira (2010) defendem que “[…] mensagens contendo ameaças e calúnias são muito comuns. Em outros casos, denúncias são realizadas devido a e-mails que tentam enganar os destinatários, roubando-lhes informações. [...]”.

Uma conta de e-mail fictícia cria inúmeras possibilidades para crimes. Segundo Costa (2011) um e-mail fictício é como uma identidade falsa que dá suporte a todo tipo de ato ilícito praticado por ele.

Segundo o “Relatório de Ameaças à Segurança na Internet” da Symatec (2014) os ataques direcionados, ou *Spear-Phishing*, têm crescido bastante apesar de o público por campanha ter diminuído bastante. Isso se deve a uma mudança de foco no público-alvo. Hoje, as empresas de pequeno e médio porte são as mais ameaçadas, chegando a ocupar 61% dos alvos de ataque em 2013. Conforme podemos ver na Figura 01.

Figura 01 – Evolução dos ataques baseados em *Spear-Phishing*



Fonte: Symantec (2014)

2.4 ANÁLISE FORENSE DE MENSAGENS DE CORREIO ELETRÔNICO

A análise de e-mails consiste não somente na leitura da mensagem recebida, pois nos casos onde a natureza da mensagem é ilícita é muito comum que o remetente seja falso ou forjado. Identificar o autor é uma tarefa que consiste principalmente na análise do cabeçalho do e-mail. O cabeçalho de um e-mail contém informações sobre o caminho percorrido pela mensagem desde a sua origem. Segundo Costa (2011), em um processo de envio de e-mail adiciona-se pelo menos três cabeçalhos que servem para identificar as máquinas ou servidores por onde ele trafegou. Um exemplo de cabeçalho de correio eletrônico será demonstrado na Figura 02.

Conforme pode ser visto na Figura 02, é possível identificar o endereço IP do remetente e dos servidores por onde a mensagem trafegou. Segundo Eleutério, Pedro Monteiro da Silva e Machado, Márcio Pereira (2010) por meio do endereço IP contido nestes campos é possível, com o uso de técnicas, ou ainda dos *logs* dos provedores de *internet*, identificar os responsáveis pelo envio da mensagem.

Figura 02 – Exemplo de um cabeçalho de e-mail

```
Delivered-To: givailson@gmail.com
Received: by 10.76.103.141 with SMTP id fw13csp3168835oab;
        Sun, 17 May 2015 06:01:55 -0700 (PDT)
X-Received: by 10.236.1.198 with SMTP id 46mr18405065yhd.182.1431867714701;
        Sun, 17 May 2015 06:01:54 -0700 (PDT)
Return-Path: <bounce-mc.us9_34254429.676973-givailson=gmail.com@mail23.atl161.mcsv.net>
Received: from mail23.atl161.mcsv.net (mail23.atl161.mcsv.net. [198.2.138.23])
        by mx.google.com with ESMTP id u70si4382230yhp.8.2015.05.17.06.01.54
        for <givailson@gmail.com>;
        Sun, 17 May 2015 06:01:54 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce-mc.us9_34254429.676973-
givailson=gmail.com@mail23.atl161.mcsv.net designates 198.2.138.23 as permitted sender)
client-ip=198.2.138.23;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of bounce-mc.us9_34254429.676973-
givailson=gmail.com@mail23.atl161.mcsv.net designates 198.2.138.23 as permitted sender)
smtp.mail=bounce-mc.us9_34254429.676973-givailson=gmail.com@mail23.atl161.mcsv.net;
       dkim=pass header.i=@mail23.atl161.mcsv.net
```

Fonte: Gmail(2015)

2.5 O QUE MUDOU NA ANÁLISE DE E-MAIL COM A LEI Nº 12.965

A Lei Nº 12.965, de 23 de Abril de 2014, também conhecida como “Marco Civil da *Internet*” foi criada para regular os direitos e deveres de usuários, e também dos prestadores de serviço. De acordo com Costa (2011), em publicação anterior a lei, poderiam haver situações onde a localização não seria possível mesmo de posse dos dados suficientes. A identificação do responsável poderia ser frustrada pela falta de norma reguladora, que obriga a guarda dos *logs* de acesso.

Contudo, o “Marco Civil da *Internet*” em seu artigo 15 define o prazo de 6 (seis) meses para a guarda dos *logs* de acesso, desde que estejam sob sigilo em ambiente controlado e de segurança. E define, também, que as autoridades policiais, administrativas e ainda o Ministério Público poderão requerer cautelarmente esses dados de qualquer provedor, inclusive nos casos onde o prazo exceda o tempo previsto de seis meses.

3 METODOLOGIA E MATERIAIS

3.1 CLASSIFICAÇÃO (TIPOS) DA PESQUISA

A pesquisa sobre o tema foi realizada por meio de consulta a literatura especializada em investigação forense e a sites de normatização das tecnologias para a web, bem como lei governamental que se aplica ao tema.

Para a realização da classificação da pesquisa foi utilizado os conceitos de PRODANOV e ERNANI (2013) e alguns artigos, identificando-se os tipos científicos a seguir:

a) Quanto à natureza - Pesquisa aplicada: Com a explicação dos processos de envio e analise de um e-mail, o presente artigo fornece o conhecimento básico necessário a ser usado em uma analise forense.
b) Quanto à natureza objetiva – Pesquisa exploratória: Através de uma pesquisa aprofundada que envolve várias áreas, o presente artigo procura fornecer uma visão ampla, garantindo um completo entendimento sobre o tema apresentado.

c) Quanto à natureza técnica – Estudo de caso: Através de uma análise de e-mail faz-se a aplicação dos conhecimentos levantados durante o desenvolvimento deste artigo.

3.2 INSTRUMENTOS E PROCEDIMENTOS

3.2.1 Estudo de caso

Com base nos conceitos aqui apresentados, serão criadas duas contas de e-mail, uma no *Yahoo* e outra no *Gmail*. Estas contas terão o propósito de exemplificar o processo de envio de um e-mail padrão.

Em um segundo momento um e-mail de natureza anônima será enviado para a conta do *Gmail*. Neste procedimento será utilizado um serviço online de envio anônimo, que encontra-se disponível de modo gratuito, em https://www.guerrillamail.com/inbox e foi escolhido pois faz uso de contas de e-mail descartáveis, não necessitando do fornecimento de quaisquer dados do usuário remetente para a realização do envio da mensagem.

As mensagens serão analisadas em sua estrutura de cabeçalho, com o objetivo de encontrar informações de IP de origem da máquina ou roteador e destacados somente os campos que utilizaremos para demonstrar a origem de cada uma, sendo eles: ***Received*** e ***X-Originating-IP***. Costa (2011), os assim definem:

a) ***Received***: este campo identifica o servidor por onde a mensagem passou. Um e-mail deverá conter, nos campos *Received,* todos os endereços das máquinas por onde ele trafegou; e
b) ***X-Originating-IP***: contém o endereço IP do remetente e, normalmente, é preenchido por clientes de *webmail* como é o caso do *Hotmail*.

Durante o processo de identificação serão informados, com o auxílio de literatura especializada, os passos a serem tomados para cada impedimento que possa ocorrer.

3.3 CRIAÇÃO DAS CONTAS DE E-MAIL E DISPARO DE MENSAGENS

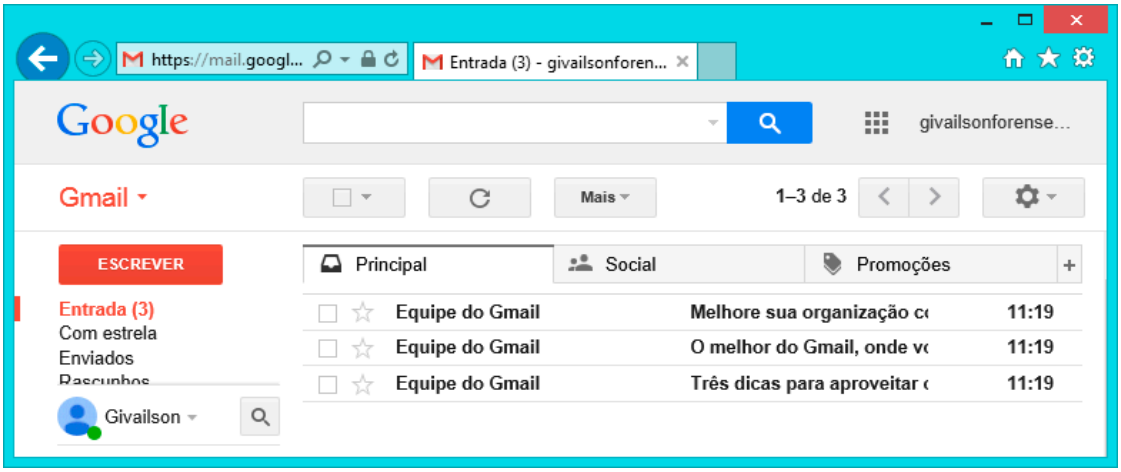
Acessando o portal do *Gmail* e preenchendo, com dados válidos, o formulário de criação de e-mail foi criada a conta givailsonforense@gmail.com.br, conforme pode ser visto na Figura 03.

Em seguida, procedimento similar foi realizado no portal do *Yahoo* para a criação da conta givailsonforense@yahoo.com.br, conforme pode ser visto na Figura 04.

Após a criação das contas, um e-mail de exemplo foi criado na conta do *Gmail* e enviado para a conta do Yahoo, conforme será demonstrado na Figura 05.

Acessando o site https://www.guerrillamail.com/inbox, e preenchendo apenas os campos de destinatário um e-mail foi enviado deste site para a conta givailsonforense@gmail.com. Este procedimento pode ser visto na Figura 06. Para finalizar o envio desta mensagem, foi solicitada uma validação que tem o objetivo de verificar se o usuário não é um robô.

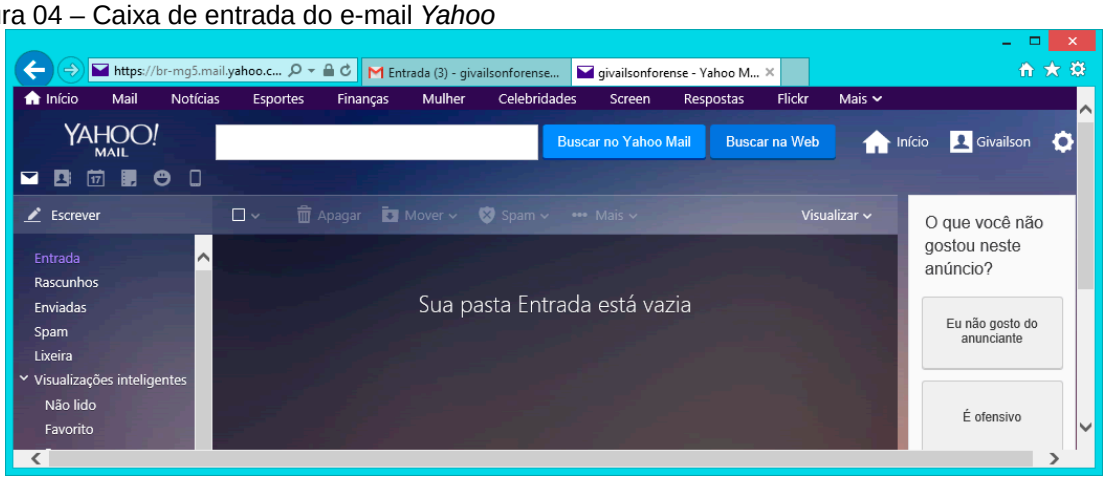
Figura 03 – Caixa de entrada do *Gmail*



Fonte: Gmail(2015)

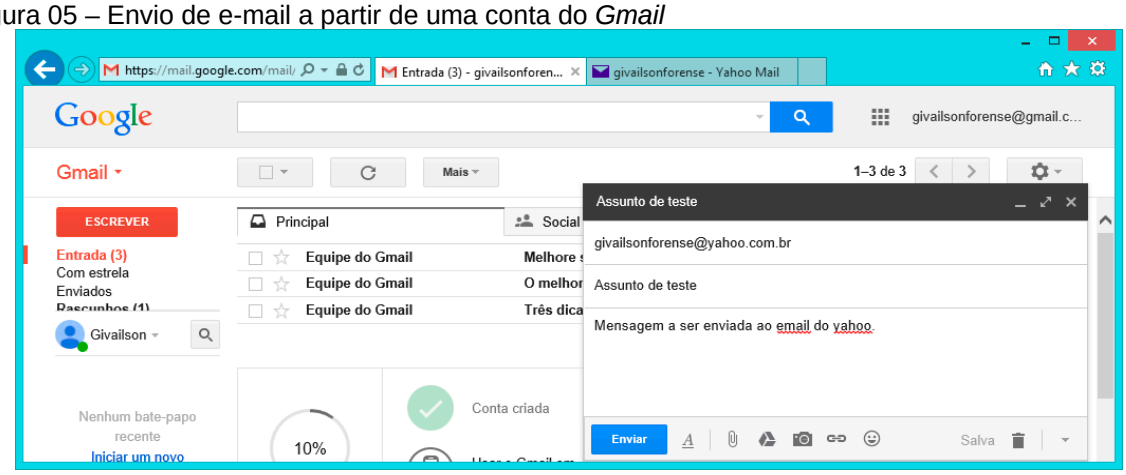
Ambos os e-mails foram corretamente recebidos pelos destinatários nas respectivas caixas de entrada. E apesar do remetente, gerado pela ferramenta de disparo anônimo, ser um tanto estranho aos olhos humanos (19t3e7+7y3s2cvzgqk90@sharklasers.com). O *Gmail* não fez nenhuma objeção ou marcação, indicando que a mensagem pudesse ser de origem suspeita.

Figura 04 – Caixa de entrada do e-mail *Yahoo*



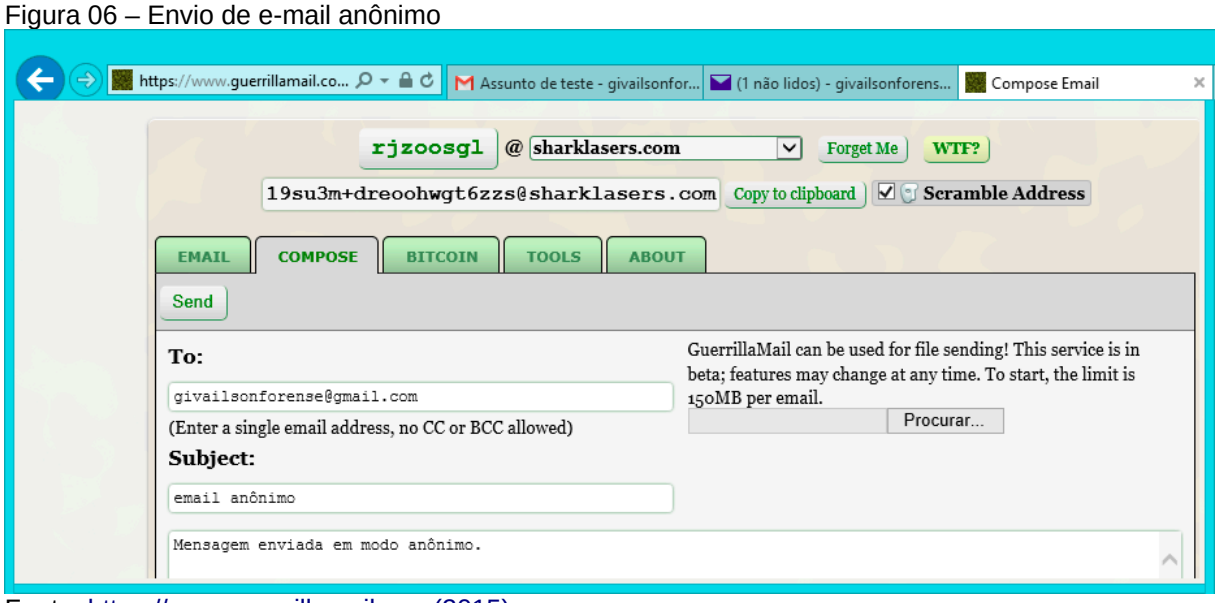
Fonte: *Yahoo mail(2015)*

Figura 05 – Envio de e-mail a partir de uma conta do *Gmail*



Fonte: *Gmail(2015)*

Figura 06 – Envio de e-mail anônimo



Fonte: https://www.guerrillamail.com(2015)

3.4 ANALISANDO A ORIGEM DO E-MAIL ENVIADO DE MANEIRA PADRÃO

Na página inicial do Yahoo, após localizar e abrir o e-mail que foi enviado pela conta givailsonforense@gmail.com usando o botão **Exibir cabeçalho completo** no menu **mais**, a direita do topo da mensagem, uma janela *pop-up* será exibida contendo os valores do cabeçalho, conforme poderá ser visualizado na Figura 07.

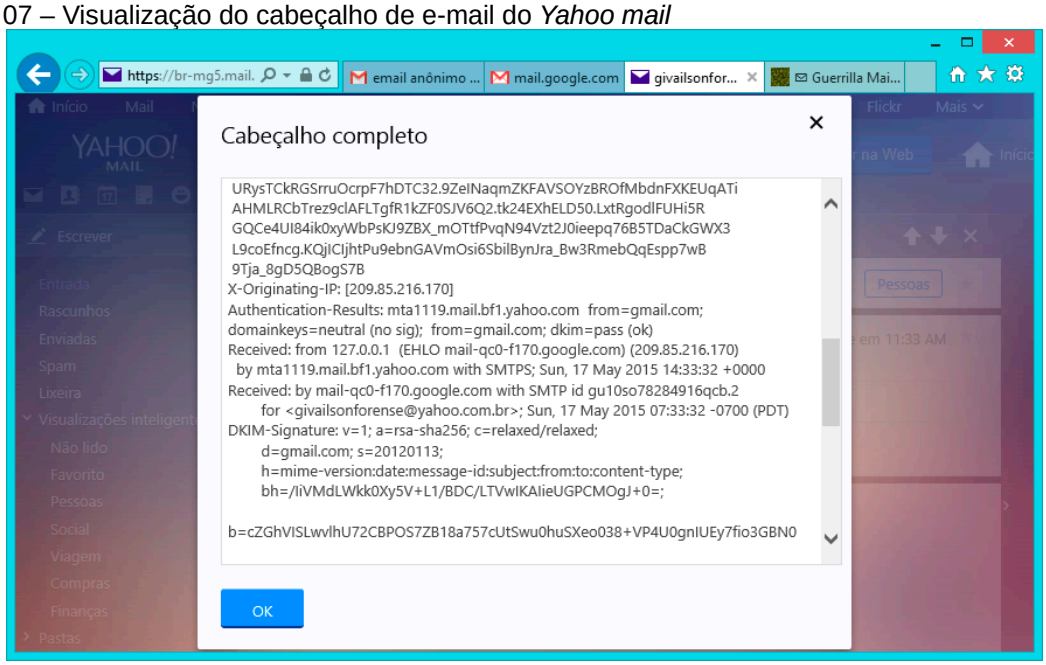
Nela pode-se ver que os campos ***Received*** e ***X-Originating-IP***, contêm o mesmo valor de endereço IP [209.85.216.170]. O que pode indicar que o *Gmail* oculta o IP da máquina de origem do usuário.

3.5 ANALISANDO A ORIGEM DO E-MAIL ANÔNIMO

Com o e-mail anônimo aberto, será selecionado a opção **mostrar original** disponível no *menu* **mais**, que encontra-se a direita das informações de remetente. Este procedimento, específico do *Gmail*, abrirá uma nova aba do navegador onde será exibida a mensagem com todos os cabeçalhos a vista. A janela que contém essas informações poderá ser visualizada na Figura 08.

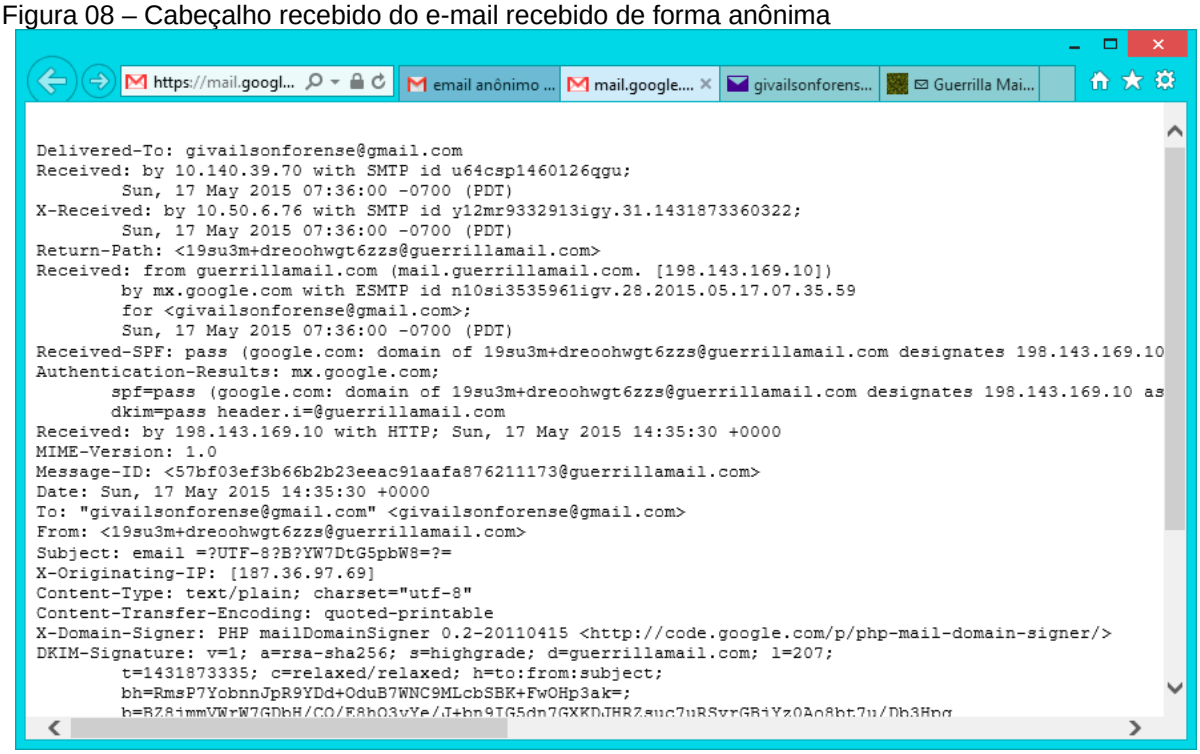
Na Figura 08 veremos que a incidência do campo ***Received*** indica o site que foi utilizado para realizar o disparo, pois o valor após os dois pontos indica ***from*** **guerrillamail.com (mail.guerrillamail.com. [198.143.169.10])**. Por este campo já seria possível identificar o local onde a mensagem foi criada. Contudo, indo mais a fundo e verificando o campo ***X-Originating-IP***, nos deparamos com o endereço IP **187.36.97.69**, que identifica a máquina de origem ou o roteador utilizados para acessar a *internet* e fazer o envio do e-mail anônimo.

Figura 07 – Visualização do cabeçalho de e-mail do *Yahoo mail*



Fonte: *Yahoo mail(215)*

Figura 08 – Cabeçalho recebido do e-mail recebido de forma anônima



Fonte: *Gmail(2015)*

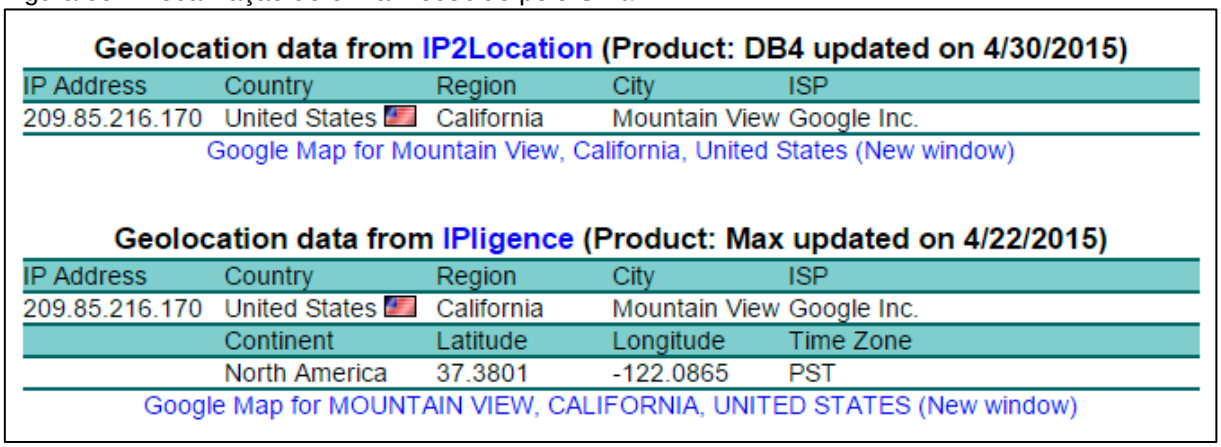
4 RESULTADOS

Com base nas informações colhidas será procedida uma tentativa de localizar a origem da mensagem. Este passo terá por base um serviço online gratuito, disponível em http://www.iplocation.net/ que terá o propósito de demonstrar o quão preciso pode ser a localização baseada no endereço IP encontrado recuperado.

4.1 RESULTADOS DA ANALISE DO E-MAIL ENVIADO DE MANEIRA PADRÃO

Conforme pode ser visto na Figura 09, tanto o servidor quanto a máquina de origem inicial estão direcionados para a sede do *Google* na Califórnia. Segundo Eleutério, Pedro Monteiro da Silva e Machado, Márcio Pereira (2010), quando essa situação ocorrer, onde a autoria do e-mail é direcionada ao provedor do serviço, a autoridade competente de posse dos dados do cabeçalho, deverá contatar a empresa prestadora do serviço de e-mail para poder localizar IP que gerou a mensagem. A partir da obtenção destes dados, novos procedimentos poderão ser tomados até que se chegue à fonte do e-mail.

Figura 09 – Localização do e-mail recebido pelo *Gmail*



Geolocation data from IP2Location (Product: DB4 updated on 4/30/2015)

IP Address	Country	Region	City	ISP
209.85.216.170	United States	California	Mountain View	Google Inc.

Google Map for Mountain View, California, United States (New window)

Geolocation data from IPligence (Product: Max updated on 4/22/2015)

IP Address	Country	Region	City	ISP
209.85.216.170	United States	California	Mountain View	Google Inc.
	Continent	Latitude	Longitude	Time Zone
	North America	37.3801	-122.0865	PST

Google Map for MOUNTAIN VIEW, CALIFORNIA, UNITED STATES (New window)

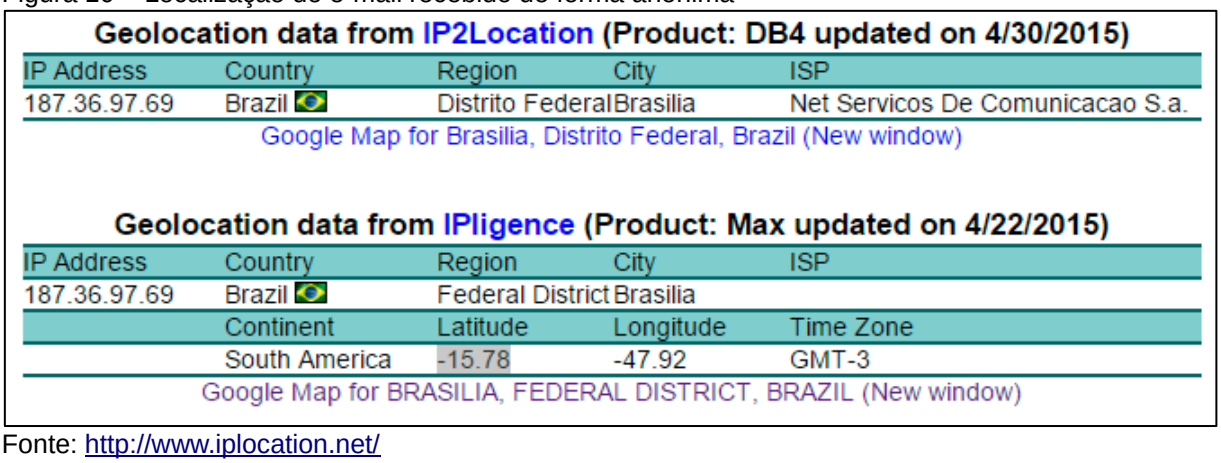
Fonte: http://www.iplocation.net/(2015)

4.2 RESULTADOS DA ANALISE DO E-MAIL ENVIADO DE MANEIRA ANÔNIMA

O endereço IP obtido, como feito no caso anterior, será utilizado no serviço de geolocalização. A Figura 10 mostrará os resultados obtidos.

Na Figura 10, foi possível localizar a cidade a posição global e até a empresa provedora do serviço de internet. Segundo Eleutério, Pedro Monteiro da Silva e Machado, Márcio Pereira (2010) de posse do endereço IP, data e hora (com fuso horário) será possível contatar o provedor de internet e identificar o usuário responsável pela mensagem, bem como o seu endereço.

Figura 10 – Localização do e-mail recebido de forma anônima



Geolocation data from IP2Location (Product: DB4 updated on 4/30/2015)

IP Address	Country	Region	City	ISP
187.36.97.69	Brazil	Distrito Federal	Brasilia	Net Servicos De Comunicacao S.a.

Google Map for Brasilia, Distrito Federal, Brazil (New window)

Geolocation data from IPligence (Product: Max updated on 4/22/2015)

IP Address	Country	Region	City	ISP
187.36.97.69	Brazil	Federal District	Brasilia	
	Continent	Latitude	Longitude	Time Zone
	South America	-15.78	-47.92	GMT-3

Google Map for BRASILIA, FEDERAL DISTRICT, BRAZIL (New window)

Fonte: http://www.iplocation.net/

4.3 COMPARAÇÃO DE RESULTADOS

Conforme pode ser observado neste estudo de caso, alguns serviços que prometem o anonimato deixam passar informações preciosas sobre a autoria e origem da informação, pois, aparentemente, será mais trabalhoso chegar ao usuário que enviou um e-mail malicioso com uma conta falsa no *Gmail*. Em ambos os casos o estudo do cabeçalho é uma peça-chave para as investigações, visto que os dados lá contidos ou trarão a correta localização ou fornecerão insumos ao próximo passo da investigação.

5 CONCLUSÃO

Como visto, muitas são as ameaças que circundam os usuários de e-mail nos tempos atuais. Isso sem falar nos criminosos que utilizam o e-mail como forma de disseminar conteúdo ilícito. Apesar de o e-mail ser similar a uma identidade na *internet*, o processo de localizar o responsável pela mensagem por vezes não é tão simples. Determinar a localização exata do envio da mensagem e o responsável requer tanto um conhecimento técnico quanto o conhecimento de leis e procedimentos. Criar um e-mail falso ou ainda usar uma ferramenta de anonimato não requer muito trabalho. Este procedimento pode levar poucos minutos, talvez por isso seja crescente o número de fraudes efetuadas por este meio.

Após a identificação dos processos envolvidos no envio de uma mensagem de correio eletrônica, não é difícil perceber o quanto é importante o conhecimento das informações presentes em um cabeçalho de e-mail e como elas são a chave para a correta identificação do responsável, pois guardam informações como: IP, data e hora das transmissões da mensagem. Com o advento do “Marco civil da *Internet*”, que obriga os provedores de serviço de internet a guardarem informações de acesso por seis meses, no mínimo. O IP contido nos cabeçalhos foi reafirmado como peça-chave na localização do responsável.

Ficou claro por meio do estudo de caso apresentado, que é possível verificar até os e-mails enviados por serviços que afirmam garantir o anonimato do remetente, e que de certa forma eles acabam sendo menos anônimos dos que não fazem este tipo de propaganda. Alguns serviços de anonimato além de identificar o servidor utilizado, não ocultam o IP de origem do usuário. Diferentemente dos servidores convencionais, como é o caso do *Gmail*, que requererão processos mais complexos para identificar o responsável pela mensagem, devido ao fato de ocultar o endereço da origem.

Apesar de existir um padrão definido, a forma com que os dados são expostos nos cabeçalhos pode variar de servidor para servidor. Cabe ao perito não fazer conclusões precipitadas com pequenas partes do das informações encontradas. O cabeçalho de um e-mail deve ser analisado como um todo, verificando todos os servidores por onde a imagem trafegou até a sua origem. Somente com esse processo cauteloso será possível localizar a fonte da mensagem.

Outro complicador que pode ser utilizado pelos criminosos digitais é o modo de navegação anônimo como a rede **Tor**. Quando um usuário faz uso deste meio, fica quase impossível detectar a origem do e-mail. Nestes casos o cabeçalho não será tão útil, porém isso ainda não retira a necessidade de seu conhecimento, visto que nem todo o criminoso faz uso ou tem conhecimento dessas tecnologias.

5.1 TRABALHOS FUTUROS

Para amplificar o conhecimento aqui levantado sugiro o aprofundamento dos processos legais envolvidos na identificação da autoria de um e-mail. Para isso pode-se fazer uso de casos conhecidos e julgados nos tribunais de justiça. Este aprofundamento irá garantir um melhor detalhamento sobre os processos finais da investigação da autoria de um e-mail.

6 RESUMO EM LÍNGUA ESTRANGEIRA

ANALYSIS AND IDENTIFICATION OF E-MAIL AUTHORSHIP

Abstract:
There are many threats that surround the e-mail users in modern times. Data capture and malicious software installations are just a few examples where there may be direct attacks on users. Not to mention the criminals who use e-mail as a way to disseminate illegal content, such as pedophiles. This paper detailed the process of sending and receiving an email and how knowledge of basic composition of his header is important for a forensic expert. To carry out this empirical study was conducted exploratory research, based, applied research, literature and case study about the history of e-mail, its composition and the means with which an expert normally account for the location of the sender. After a case study involving the header of two emails, sent a standard and another anonymously made it possible to check the location of authorship and the steps needed to Sender identification.

Keywords: E-mail. E-mail. Forensic Computing. Eletronic fraud.

7 REFERÊNCIAS

BRASIL. **Lei Nº 12.965, de 23 de abril de 2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 17 maio 2015

COSTA, Marcelo Antônio Sampaio Lemos. **Computação Forense**. São Paulo: Millennium, 2011. p. 147.

ELEUTÉRIO, Pedro Monteiro da Silva e MACHADO, Márcio Pereira. **Desvendando a computação forense**. São Paulo: Novatec, 2010. p. 197.

GOODRICH, Michael T. & TAMASSIA, Roberto. **Introdução à segurança de computadores**. Porto Alegre, 2013. p 550.

IETF. Request for Comments 5322 – **Internet Message Format**. Disponível em: <http://tools.ietf.org/html/rfc5322>. Acesso em: 06 Abril 2015.

PRODANOV, Cleber Cristiano e Freitas, ERNANI, Cesar de. **Metodologia do trabalho científico**. Rio Grande do Sul: Universidade FEEVALE. 2013. p. 276.

SYMANTEC. **Relatório de Ameaças à Segurança na Internet de 2014**, Volume 19, Symantec. Disponível em:<https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf>. Acesso em: 07 Abril. 2015.