Rastreamento de E-mails

Conteúdo extraído de: <http://www.infocrime.com.br/category/e-mails>
Autor: Marcelo Sampaio

Sumário

Extraindo cabeçalhos de mensagens de e-mail

O rastreamento de *e-mails* exige a realização de uma análise no cabeçalho completo (*e-mail header*) da mensagem investigada. O cabeçalho completo é um relatório que começa a ser criado na composição da mensagem e a medida que é transmitido entre os diversos servidores recebe novos campos contendo informações sobre a rota traçada até o seu destino final. O conteúdo destes cabeçalhos também permite que se examine a autenticidade da mensagem e a identificação dos campos de rastreamento, determinando se um ou mais campos foram forjados e se as informações extraídas possibilitam a identificação da origem e da autoria.

Assim além do corpo da mensagem é necessário se obter o cabeçalho completo, e isso só é possível obtendo a mensagem a partir de um destinatário direto do *e-mail*, ou seja, dos destinatários originais da mensagem. Portanto não se presta para a análise o encaminhamento de seu conteúdo, pois só o corpo da mensagem é enviado e o cabeçalho completo é substituído pelos do processo de encaminhamento.

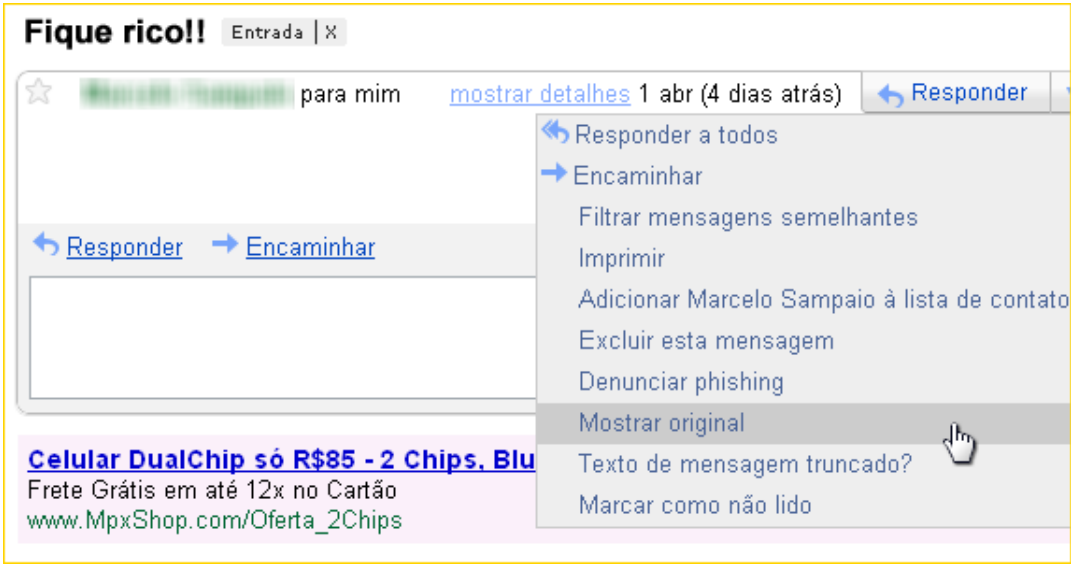
Existe uma grande diversidade de clientes de *e-mail* e *webmail*, que são frequentemente atualizados, criando alguma dificuldade na localização do acesso ao cabeçalho completo da mensagem.

Este texto tem como propósito auxiliar a localização e cópia dos cabeçalhos e códigos fontes das mensagens, preservando-as para a produção da prova material.

Webmails

Gmail, IG, SuperIG, iBest, BRTurbo, Oi, etc. (powered by google)

Acesse a conta do *Gmail* e abra a mensagem a qual deseja visualizar o cabeçalho. Na janela que mostra o conteúdo da mensagem clique no menu situado na porção superior direita da janela da mensagem, que exibe por padrão a opção *Responder* e selecione a opção *Mostrar original*. Selecione todo o conteúdo e salve-o em um arquivo com a extensão *TXT* ou *EML*. O formato *EML* (acrônimo de *Eletronic Mail*) é um formato comum a vários clientes de correio e seu conteúdo mostra o cabeçalho completo e o corpo da mensagem e como o *TXT*, pode ser aberto com qualquer editor de texto *ASCII*.



Hotmail

No *Windows Live Hotmail* são oferecidas duas alternativas. Na primeira vá para a mensagem desejada, clique com o botão direito do *mouse* sobre a mesma e selecione no menu de contexto que se abre, a opção *Exibir o código-fonte da mensagem*. Na segunda opção abra a mensagem e clique na seta do menu situado na porção superior direita da janela da mensagem, que exibe por padrão a opção *Responder* (como no *Gmail*) e selecione a opção *Exibir o código-fonte da mensagem*. Selecione todo o conteúdo e salve-o em um arquivo com a extensão *TXT* ou *EML*.

Yahoo Mail e YMail (Novo Yahoo)

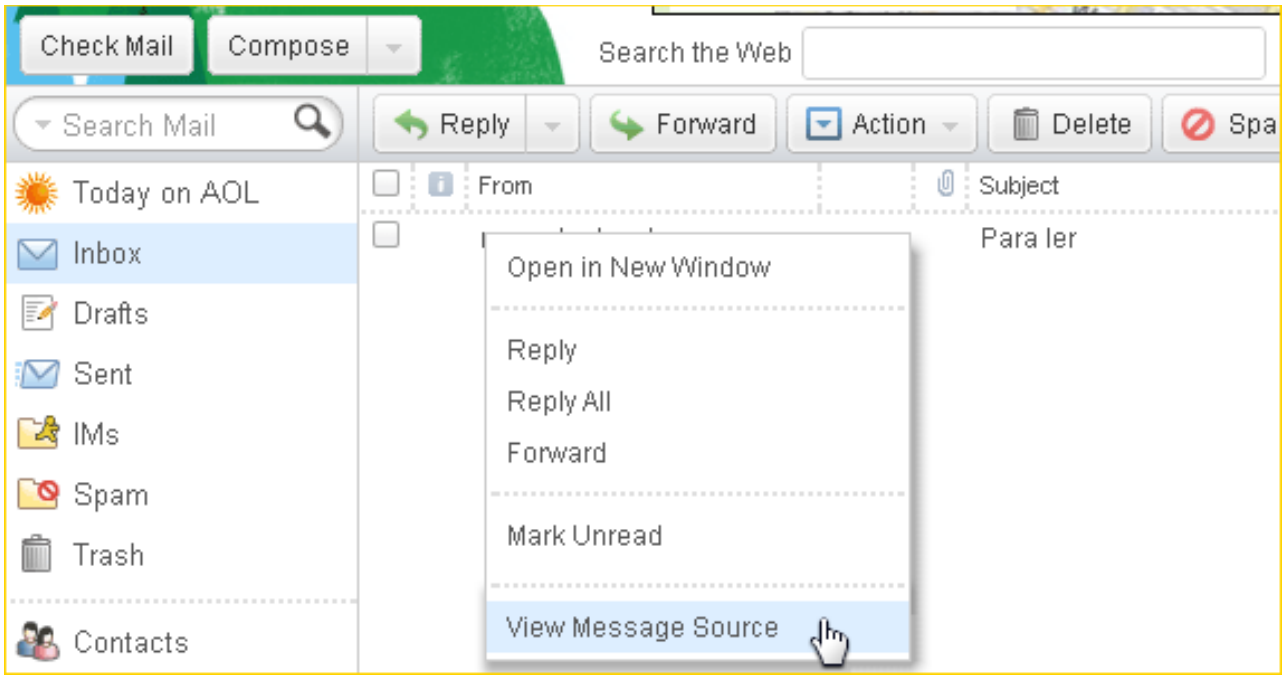
Como o *Hotmail*, o *Yahoo* também oferece três maneiras de se chegar ao conteúdo do cabeçalho completo da mensagem. Conecte-se à conta de *e-mail* do *Yahoo* e clique com o botão direito sobre a mensagem desejada, selecione no menu de contexto que se abre, a opção *Exibir cabeçalho completo*. Na segunda, clique sobre o botão *Ações* e selecione *Exibir cabeçalho completo.* Por fim abra a mensagem e no botão *Ações*, selecionado em seguida a opção *Exibir cabeçalho completo*. Selecione todo o conteúdo e salve-o em um arquivo com a extensão *TXT* ou *EML*.

BOL e UOL

Conecte-se na conta de *e-mail* do *BOL* ou *UOL* e clique sobre a mensagem desejada. No painel de visualização da mensagem situado abaixo da lista de mensagens, clique sobre o botão *Mais ações…* selecionando neste menu a opção *Ver o código* ou *Exportar (eml).* Ao exibir o código selecione o conteúdo e salve-o como arquivo com a extensão *TXT* ou *EML*. Se optar por *Exportar (eml)* o arquivos será salvo em formato *EML*.

AOL

Conecte-se na conta de *e-mail* da *AOL* e clique com botão direito do *mouse* sobre a mensagem desejada e selecione no menu de contexto a opção *View Message Source.* Selecione todo o conteúdo e salve-o em um arquivo com a extensão *TXT* ou *EML*.



Clientes de correio

Outlook 2007 e 2010

Para acessar os cabeçalhos completos das mensagens no *Microsoft Outlook 2007*, cliente de correio que integra a suíte do *Microsoft Office*, clique com o botão direito do *mouse* sobre a mensagem desejada, selecione no menu de contexto que se abre a opção *Opções da mensagem…* Na porção inferior da janela que se abre, em *Cabeçalhos da Internet:* é possível visualizar o conteúdo do cabeçalho completo da mensagem. Selecione todo o conteúdo e salve-o em um arquivo texto.

No *Microsoft Outlook 2010* abra a mensagem desejada e clique na guia *Arquivo* situada na aba mais à direita. Em *Informações* clique sobre a opção *Propriedades.* Na porção inferior da janela que se abre, em *Cabeçalhos da Internet:*, é possível visualizar o conteúdo do cabeçalho completo da mensagem. Selecione todo o conteúdo e salve-o em um arquivo texto.

Em ambos pode-se salvar a mensagem com a extensão *msg* e depois convertê-la para o formato texto para análise.

Outlook Express e Windows Live Mail 2011

Estes dois clientes de correio eletrônico da *Microsoft* possuem procedimentos de visualização dos cabeçalhos da mensagem idênticos, com acesso ao conteúdo em dois estágios diferentes. Clicando com o botão direito do *mouse* sobre a mensagem desejada, selecione no menu a opção *Propriedades*. Na janela que se abre selecione a guia *Detalhes* e poderá visualizar o conteúdo do cabeçalho completo da mensagem. Caso queira ter acesso ao código-fonte da mensagem clique sobre o botão *Código-fonte da mensagem…* nesta janela. Outra opção é selecionar a mensagem desejada e no menu *Arquivo* selecione a opção *Salvar Como.* Em seguida escolha o formato *EML* e salve o arquivo.

Incredimail 2.0

Para acessar o conteúdo do cabeçalho no *Incredimail*, abra a mensagem desejada e vá ao menu *Arquivo*, selecionado a opção *Propriedades* e na janela que se abre escolha a aba *Detalhes*. Selecione todo o conteúdo e salve-o em um arquivo texto. Outra forma é selecionar a mensagem desejada e no menu *Arquivo* selecione a opção *Salvar Como.* Em seguida escolha o formato *EML* e salve o arquivo.

Thunderbird 3.1.6

Para acessar o conteúdo do cabeçalho no cliente de correio eletrônico da *Mozilla Foudation*, selecione a mensagem desejada e na janela de visualização situada abaixo da lista de mensagens, abra o menu situado no botão *outras ações* situado à esquerda desta e selecione a opção *exibir código-fonte*. Outra opção é selecionar a mensagem desejada e no menu *Arquivo* selecione a opção *Salvar como arquivo…* Em seguida escolha o formato *EML* e salve o arquivo.

Eudora 7.0 e OSE 1.0

No *Eudora* 7.1 abra a mensagem desejada e clique na barra de ferramentas no ícone *Blah Blah*, copie o conteúdo e salve em um arquivo *TXT* ou *EML*. No *Eudora OSE 1.0* selecione a mensagem desejada e na barra central role para baixo e clique no botão *Other actions*, selecione então a opção

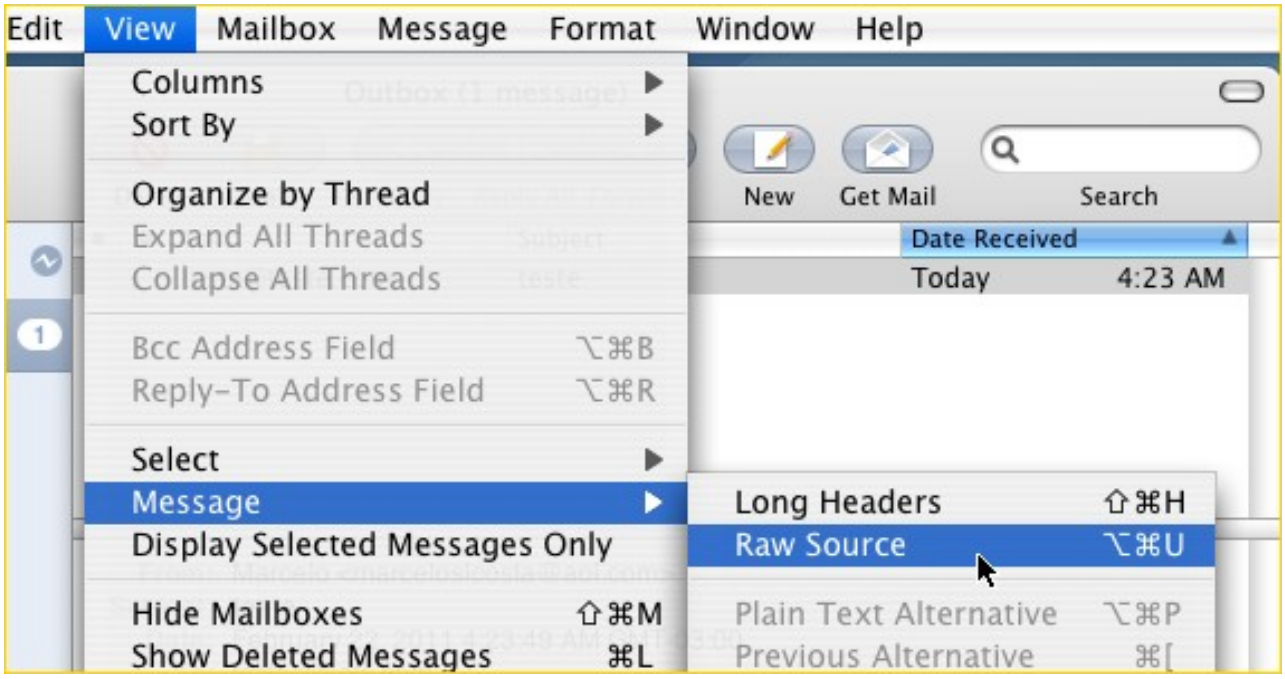
view source e salve o conteúdo da janela para um arquivo de formato *TXT* ou *EML*. Se selecionar a opção *save as…* e salve o arquivo no formato *TXT* ou *EML*.

Lotus Notes 8.5

No caso do cliente de correio da *IBM*, o *Lotus Notes*, os cabeçalhos completos de mensagens da *internet* podem ser visualizados abrindo a mensagem desejada e clicando no menu *View*, selecionando a opção *Origem da página*. Para mensagens internas vá para a lista e clique com o botão direito do *mouse* sobre a mensagem desejada e selecione no menu de contexto que se abre a opção *Propriedades do documento*.

Mail 2.0.1 (MacOS X 10)

Clique sobre a mensagem desejada, abra o menu *View*, expanda o item *Message* e selecione o item *View Source*.



Opera 11.01

O *browser Opera* possui um cliente de *e-mail* com suporte *POP* e *IMAP* embutido no navegador. Para ter acesso aos cabeçalhos das mensagens clique no menu do *Opera* e selecione a opção *Mail* para acessar o cliente de *e-mail*. Uma vez com o cliente aberto, clique com o botão direito do *mouse* sobre a mensagem desejada e selecione no menu de contexto que se abre a opção *Exibir todos os cabeçalhos e mensagem*. O código-fonte da mensagem será mostrado no painel de leitura. Selecione todo o texto, copie e cole em um arquivo *TXT* ou *EML*.

Pegasus 4.5

Clique com o botão direito do *mouse* sobre a mensagem desejada e selecione no menu de contexto que se abre a opção *Message headers*. O cabeçalho completo poderá ser visto na guia *Raw view*, copiado e salvo em um arquivo *TXT* ou *EML*.

Rastreamento de E-mails

Origem e Autoria

Vamos começar uma nova série de *posts* relativos à perícia e ao rastreamento de mensagens de correio eletrônico com fins de identificação de autoria. Porém antes de iniciar a abordagem técnica irei discutir alguns aspectos relativos à origem e autoria dessas mensagens.

Em geral se imagina que para descobrir **quem** enviou um *e-mail*, basta identificar o endereço *IP* do remetente e pronto. Mas não é bem assim que a coisa funciona. Primeiramente "**quem**" está relacionado ao autor e o endereço *IP* está diretamente associado ao "onde" e ao "quando", podendo chegar até ao "que" e ao "como", mas determinar o "quem" pode ser bem mais complexo.

A determinação de origem e de autoria de e-mails são dois processos distintos e o sucesso de ambos depende de diversos fatores como recursos tecnológicos, conhecimentos técnicos e uma coleta de dados adequada, que resultarão em uma boa qualidade das informações a serem analisadas.

A origem é a combinação do "onde" e do "quando" e está associada ao circuito físico que estabelece a conexão durante um determinado intervalo de tempo, seja ele um circuito dedicado de dados, uma linha telefônica fixa como a *ADSL* ou uma conexão *GSM*. A determinação da origem nos levará até a extremidade de um destes circuitos, entretanto o autor poderá não mais estar lá.

A autoria é o "quem" e está associada diretamente ao agente que produz a mensagem e ao dispositivo utilizado como meio (o "que"). Este dispositivo pode ser o computador de um provedor de serviços como uma *lan house*, um *cybercafé*, ou ainda um computador doméstico, um telefone móvel, um *notebook* ou qualquer outro dispositivo que tenha capacidade de conexão à *web* e envio de mensagens de correio eletrônico. O "como" é caracterizado pelo meio de composição e envio da mensagem, indo de um *software* cliente, passando por uma aplicação web, como um *webmail*.

Os registros dos dados das conexões realizados pelos provedores de acesso possibilitam a caracterização da conexão, a determinação da origem e em alguns casos específicos, quando existem provas acessórias, a autoria das mensagens. Portanto identificar o *IP* do remetente de uma mensagem poderá levar-lhe até a origem, mas pode não levar ao autor. Suponha que a mensagem foi enviada de uma *lan house* de bairro que não faz cadastro dos usuários, sem sistema de CFTV, como poderemos identificar o autor se só a utilizou uma única vez, para aquele fim específico?

O Brasil, até o presente momento, não possui uma legislação que regulamente o provimento de acesso à *internet*. Em outras palavras, os prestadores de serviços de acesso à *internet* (provedores) não são obrigados por lei, a guardar os registros de conexão de seus usuários. Isso significa que, mesmo após recuperar todos os dados necessários para se identificar a origem de uma conexão, não é garantido que essa identificação ocorrerá, pois o provedor de acesso poderá não dispor da informação necessária, simplesmente por não ser obrigado a mantê-la. Em alguns casos, ainda que consigamos tais informações, *cybercafés* e *lan houses* são frequentemente utilizados com o propósito de encobrir com o anonimato a autoria de um delito, já que poucas realizam registros de seus usuários.

Ao investigar uma ação delituosa, se houver outras provas, determinar a origem pode confirmar ou não, a autoria. Tomemos como exemplo um indivíduo que esteja relacionado a um crime por outras provas, entre elas um *e-mail*. Ao identificar que o suspeito é o assinante da linha telefônica associada ao *IP* originador da mensagem, estaremos chegando também na autoria. Mas se a mensagem é a única evidência e o *IP* nos leva a uma *lan house*, o que fazer?

O objetivo desta série de *posts* é discutir os aspectos que envolvem a composição de uma mensagem de correio eletrônico e seu cabeçalho, estudando as possibilidades de utilização dos seus campos para auxiliar a determinação da autoria.

Componentes da mensagem

Para que uma mensagem de correio eletrônico possa ser composta, enviada e recebida é necessária a existência de quatro componentes:

1. *MUA* (*Mail User Agent*) – *Software* cliente de correio eletrônico do remetente e do destinatário da mensagem como o *Outlook*, ou o *Thunderbird*, ou ainda um *webmail*;
2. *MTA* (*Mail Transfer Agent*) – Servidores por onde passam a mensagem antes de chegar ao último servidor da cadeia, que entregará a mensagem ao destinatário;
3. *MSA* (*Mail Submission Agent*) – *É* um servidor *MTA*, só que está na extremidade inicial que submete a mensagem;
4. *MDA* (*Mail Delivery Agent*) – É um servidor como os *MTAs*, só que estão na extremidade final do fluxo da mensagem e são os responsáveis pela entrega desta para o remetente.

O *MUA* do remetente compõe a mensagem e envia para o primeiro *MTA* também denominado de *MSA*, por ser o primeiro servidor. O *MTA* adiciona informações ao cabeçalho da mensagem (*header*) e a encaminha para o *MTA* seguinte e finalmente ao *MTA* que fará a entrega, o *MDA*.

Figura 1 – Componentes do serviço de correio eletrônico

O código a seguir exemplifica a composição/envio, tráfego e recebimento de uma mensagem na forma mais simplificada, apenas para ilustrar a forma como o cabeçalho é composto. Uma estação remetente compõe a mensagem e envia ao servidor de correio do remetente, que por sua vez envia para o servidor de correio do destinatário que entrega a mensagem ao destinatário.

```
1             Delivered-To: destinatario@dominio_destinatario.org
2                 Received: from mail.dominio_remetente.org
3                           (mail.dominio_remetente.org[121.122.123.10]) by
4                           mail.dominio_destinatario.org (Postfix) with ESMTP id E95F283F9E for
5                           <destinatario@dominio_destinatario.org>;
6                           Fri, 5 Jan 2012 12:25:09 -0300 (BRT)
7                 Received: from dominio_remetente.org ([192.168.1.78]) by
8                           mail.dominio_remetente.org with (Postfix) with ESMTP id 19BA36EC0E1;
9                           Fri, 5 Jan 2012 12:25:05 -0300
10                    FROM: remetente@dominio_remetente.org
11                      TO: destinatario@dominio_destinatario.org
12                    DATE: Fri, 5 Jan 2012 12:25:01 -0300
13              Message-ID: kjhvduivifevifehv@dominio_remetente.org
14                 SUBJECT: Teste
```

Figura 2 – Cabeçalho simplificado da mensagem

As linhas em vermelho (campos **FROM:**, **TO:**, **DATE:** e **SUBJECT:**) foram inseridos pelo *software* cliente do remetente. O servidor de correio do remetente ao receber a mensagem

acrescenta as linhas em azul (campos **Received:** e **Message-ID:**) e o envia ao servidor de correio do destinatário que por sua vez acrescenta as linhas em verde (campos **Received:** e **Delivered-To:**) e entrega a mensagem ao destinatário final.

A sintaxe dos campos de cabeçalho é constituída pelo nome do campo, seguido de dois pontos.

Mas um cabeçalho real é bem mais complexo e extenso, podendo apresentar outros campos e uma quantidade de entradas bem maior, conforme veremos nos próximos *posts*.

Composição e envio

No ato da composição de uma mensagem são gerados os dados que irão ser utilizados na comunicação com o servidor de correio eletrônico e formar o início do cabeçalho da mensagem. Neste momento são criados os campos "***FROM:***", "***TO:***", "***DATE:***", "***SUBJECT:***" e "***DATA***", conforme vimos no *post* anterior. Estes campos serão preenchidos no cliente e serão utilizados ao submetê-los ao servidor de correio do remetente (*MTA/MSA*). Esta transação funciona como um diálogo entre o cliente e o servidor baseado no protocolo *SMTP* (*Simple Mail Transfer Protocol*). Este "diálogo" pode ser mais facilmente compreendido quando analisamos essa comunicação através de *TELNET*, na porta 25 (porta padrão *SMTP*). No exemplo abaixo vemos a comunicação entre um cliente e um servidor de correio baseado no seguinte cenário:
Um *host* denominado "**origem**" estabelece a comunicação por *TELNET* com um servidor de correio denominado "**dominio_remetente.org**" (*Microsoft ESMTP MAIL Service, Version: 6.0.2600.5512*), tentando se passar pelo servidor "**mail.receita.fazenda.gov.br**". A comunicação se estabelece conforme a figura abaixo:

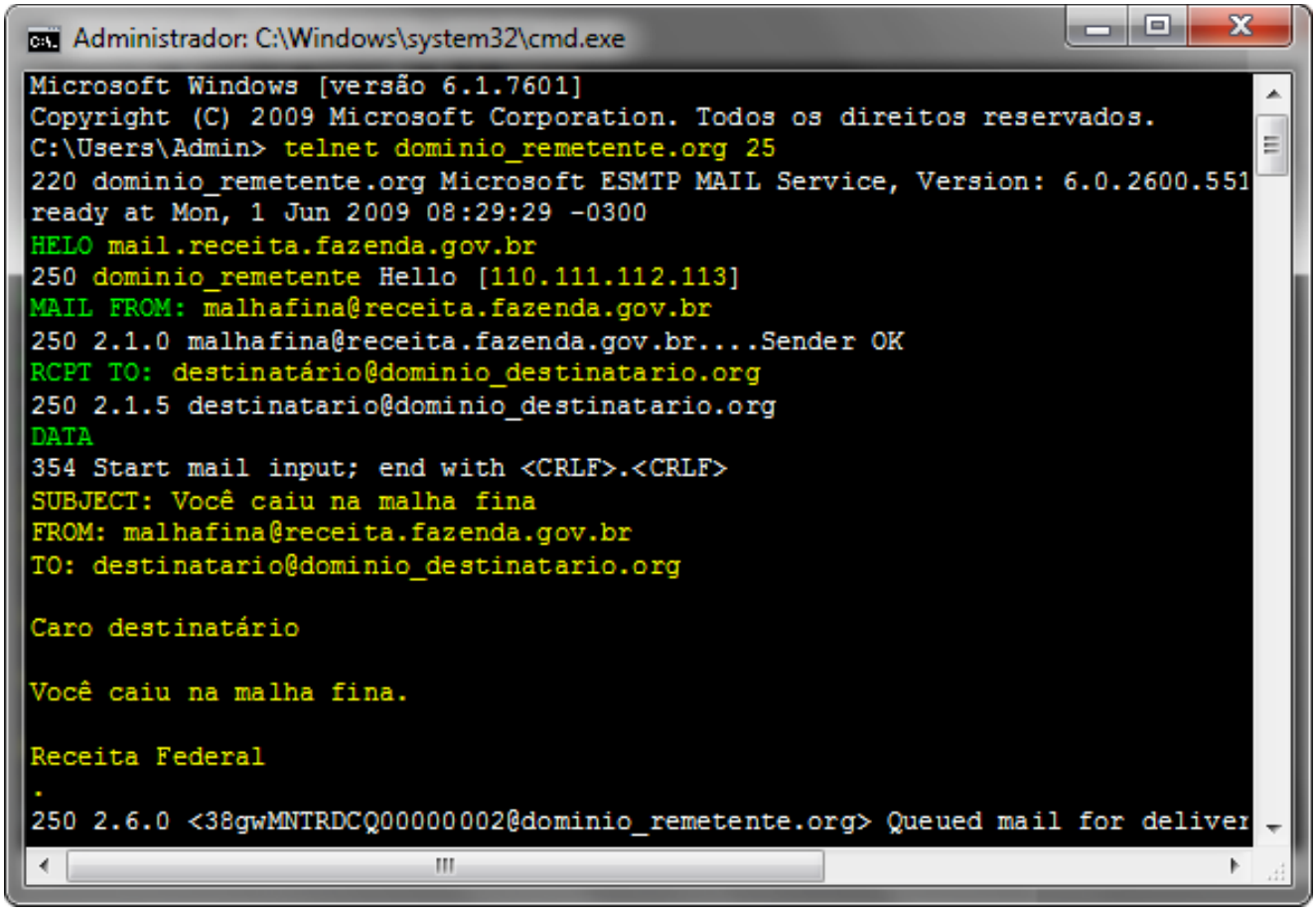


Figura 3 – Estabelecendo comunicação por TELNET (Open Relay)

Após estabelecer a conexão, repassa informações que irão fazer parte da mensagem e do cabeçalho.

```
1              Return-Path: <malhafina@receita.fazenda.gov.br>
2                 Received: from u1.dominio_destinatario.org (u1.dominio_destinatario.org
3                           [130.131.132.133]) by us5.dominio_destinatario.org (Postfix) with
4                           ESMTP id 71B941EF1C6 for <destinatario@dominio_destinatario.org>;
5                           Mon, 1 Jun 2009 08:26:35 -0300 (BRT)
6                 Received: from localhost (u1.dominio_destinatario [127.0.0.1])    by
7                           u1.dominio_destinatario.org (Postfix) with ESMTP id 09B7D99FD0 for
8                           <destinatario@dominio_destinatario.org>; Mon, 1 Jun 2009 08:39:50 -
9                           0300 (BRT)
10         X-Virus-Scanned: amavisd-new at u1.dominio_destinatario.org
11                Received: from u1.dominio_destinatario.org ([127.0.0.1])by localhost
12                          (u1.dominio_destinatario.org [127.0.0.1]) (amavisd-new, port
13                          10024)with ESMTP id VUvk9CjD for
14                          destinatario@dominio_destinatario.org>;
15                          Mon,  1 Jun 2009 08:39:44 -0300 (BRT)
16                Received: from dominio_remetente.org (dominio_remetente.org
17                          [120.121.122.123])by u1.dominio_destinatario.org (Postfix) with
18                          ESMTP id A06D79A00D for <destinatário@dominio_destinatario.org>;
19                          Mon,  1 Jun 2009 08:39:14 -0300 (BRT)
20                Received: from mail.receita.fazenda.gov.br (origem[110.111.112.113]) by
21                          dominio_remetente.org with Microsoft SMTPSVC(6.0.2600.5512); Mon, 1
22                          Jun 2009 08:30:40 -0300
23                 SUBJECT: Você caiu na malha fina
24                    FROM: malhafina@receita.fazenda.gov.br
25                      TO: destinatario@dominio_destinatario.org
26             Message-ID: <38gwMNTRDCQ00000002@dominio_remetente.org>
27   X-OriginalArrivalTime: 01 Jun 2009 11:31:25.0669 (UTC) FILETIME=[7F6A3950:01C9E2AC]
28                    Date: 1 Jan 2009 08:31:25 -0300
```

Figura 4 – Cabeçalho recebido por destinatario@dominio_destinatario.org

Como vimos antes, um *host* de nome "**remetente**" estabelece uma comunicação via *TELNET* com um servidor de correio com *relay* aberto denominado "**dominio_remetente.org**" (linha 3 da figura 3). O *host* "**remetente**" identifica-se como um *MSA* de nome "**mail.receita.fazenda.gov.br**" através do comando *HELO* ou *EHLO* (linha 6 da figura 3). Observe na linha 7 da figura 3 que "**dominio_remetente.org**" o identifica corretamente, o que também pode ser visto na linha 20 da figura 4 acima mas como está permitindo *relay*, retransmite a mensagem assim mesmo. A mensagem foi fraudada e o servidor de correio "**dominio_remetente.org**" apesar de reconhecer a diferença deixa a mensagem prosseguir, sendo que o primeiro campo "**Received:**" possui conteúdo não confiável, mas mostra a inconsistência na informação.

A composição do cabeçalho completo pode variar, agregando mais ou menos informação, entretanto se você percebe haver inconsistência em um campo "**Received:**", descarte-o e passe para o campo imediatamente acima. Os servidores seguintes estarão mais distantes do fraudador, praticamente impossibilitando que o mesmo interfira ou altere as linhas seguintes do cabeçalho.

O cabeçalho é formado à partir das linhas da base e cada *MTA* que repassa a mensagem coloca linhas acima do conteúdo recebido. Alguns campos de cabeçalho situados na base podem receber incrementos de informação, mas isso será discutido na caracterização dos campos. Até o próximo *post.*

Campos de cabeçalho

Após a composição e envio da mensagem, o cabeçalho sofre acréscimos à medida que passa pelos servidores de correio, até seu destino final. Este cabeçalho nos permite entender toda a trajetória da mensagem, desde sua origem até a entrega ao destinatário, apresentando dados que podem nos levar a determinar origem e autoria.

Abaixo vemos um cabeçalho completo originado a partir da comunicação entre dois usuários hipotéticos, "***remetente@hotmail.com***" e "***destinatário@gmail.com***" e o utilizaremos para iniciarmos a descrição dos campos mais comuns nas mensagens de correio eletrônico, o seu significado e o do seu conteúdo.

```
1            Delivered-To: destinatario@gmail.com
2                Received: by 10.112.106.198 with SMTP id gw6csp114566lbb;
3                                  Wed, 22 Feb 2012 16:35:58 -0800 (PST)
4                Received: by 10.236.190.199 with SMTP id e47mr21760082yhn.85.1329957358018;
5                                  Wed, 22 Feb 2012 16:35:58 -0800 (PST)
6             Return-Path: <remetente@hotmail.com>
7                Received: from bay0-omc1-s25.bay0.hotmail.com (bay0-omc1-s25.bay0.hotmail.com.
8                          [65.54.190.36]) by mx.google.com with ESMTP id
9                          d23si13492621anp.45.2012.02.22.16.35.57;
10           Received-SPF:         Wed, 22 Feb 2012 16:35:58 -0800 (PST)
11                         pass (google.com: domain of remetente@hotmail.com designates
12                         65.54.190.36 as permitted sender) client-ip=65.54.190.36;
13                         mx.google.com; spf=pass (google.com: domain of remetente@hotmail.com
14 Authentication-Results: designates 65.54.190.36 as permitted sender)
15               Received: smtp.mail=remetente@hotmail.com
16                         from BAY171-W83 ([65.54.190.61]) by bay0-omc1-s25.bay0.hotmail.com
17                         with Microsoft SMTPSVC(6.0.3790.4675); Wed, 22 Feb 2012 16:35:19
18                         -0800
19            Message-ID: <BAY171-W830CADCBEF9CC9977AE3A2DD650@phx.gbl>
20           Return-Path: remetente@hotmail.com
21          Content-Type: multipart/alternative;
22                         boundary="_fc338da9-6460-480f-ae0c-f59545fff555_"
23      X-Originating-IP: [111.112.113.114]
24                  From: Remetente <remetente@hotmail.com>
25                    To: <destinatario@gmail.com>
26               Subject: RE: RE: Re: RE: Boa Noite
27                  Date: Wed, 22 Feb 2012 21:35:20 -0300
28            Importance: Normal
29           In-Reply-To: <CueVCXLKMO9shg8DSa32O4mMDxg@mail.gmail.com>
30            References: <BAY171-W90A2682A6FA6EF1C1909F8DD650@phx.gbl>
31                         <CNZ5xUaNvbCD_oGZpMX7074e-Cg@mail.gmail.com>
32                         <BAY171-W950418859D7F6B71F651B4DD650@phx.gbl>
33                         <CueVCXLKMO9shg8DSa32O4mMDxg@mail.gmail.com>
34          MIME-Version: 1.0
35  X-OriginalArrivalTime: 23 Feb 2012 00:35:19.0792 (UTC) FILETIME=[055ED700:01CCF1C3]
```

Figura 5 – Cabeçalho de uma mensagem resultante de um diálogo

O campo "**From:**" contém o endereço do suposto remetente, que conforme vimos anteriormente pode ser fraudado, portanto não pode ser tomado como verdade absoluta.

O campo "**To:**" contém o endereço do destinatário que obviamente não será fraudado, já que a mensagem tem de chegar à ele. Ainda assim deverá ser observado se não corresponder com o destinatário, pois este pode ter recebido a mensagem por cópia oculta.

"**CC:**" Possui a mesma função do To: servindo para envio de cópia da mensagem a um segundo destinatário.

“**BCC:**” Significa *Bind Carbon Copy* e tem função similar ao *To:* e ao *CC:* entretanto este campo não mostra seu conteúdo, servindo para que a mensagem chegue a um terceiro destinatário sem que o destinatário principal ou o secundário saibam.

“**Subject:**” Contém o assunto da mensagem.

“**Date:**” Contém a data/hora em que a mensagem é submetida ou escrita, dependendo do sistema utilizado (*RFC 822*: *5.1*, *RFC 1123*: *5.2.14* ou *RFC 1036*: 2.1.2.).

“**MIME-Version:**” Indica que o conteúdo da mensagem foi formatado no padrão *MIME* e seu conteúdo indica qual a versão do *MIME* utilizada (*RFC 1521*).

“**Importance:**” Indica o grau de importância da mensagem (*High*, *Normal* e *Low*). É preenchido na composição e não interfere na velocidade com que a mensagem é transmitida.

“**Content-Type:**” Indica o formato do conteúdo (*RFC 1049*).

“**Return-Path:**” Utilizado na entrega final como o atributo do envelope ***MAIL FROM***.

No próximo *post* falaremos sobre campos úteis para determinação de autoria.

Até lá.

Campos de rastreio

Neste *post* vamos analisar com mais detalhes os campos de cabeçalho que podem fornecer informações importantes para a identificação de origem e autor, conhecidos como *Trace Fields* ou campos de rastreamento que são de grande importância na identificação real do remetente.

Continuaremos a utilizar o cabeçalho da figura 5 do *post* anterior como referência para os campos discutidos a seguir.

```
1            Delivered-To: destinatario@gmail.com
2                Received: by 10.112.106.198 with SMTP id gw6csp114566lbb;
3                          Wed, 22 Feb 2012 16:35:58 -0800 (PST)
4                Received: by 10.236.190.199 with SMTP id e47mr21760082yhn.85.1329957358018;
5                          Wed, 22 Feb 2012 16:35:58 -0800 (PST)
6             Return-Path: <remetente@hotmail.com>
7                Received: from bay0-omc1-s25.bay0.hotmail.com (bay0-omc1-s25.bay0.hotmail.com.
8                          [65.54.190.36]) by mx.google.com with ESMTP id
9                          d23si13492621anp.45.2012.02.22.16.35.57;
10           Received-SPF:         Wed, 22 Feb 2012 16:35:58 -0800 (PST)
11                         pass (google.com: domain of remetente@hotmail.com designates
12                         65.54.190.36 as permitted sender) client-ip=65.54.190.36;
13                         mx.google.com; spf=pass (google.com: domain of remetente@hotmail.com
14 Authentication-Results: designates 65.54.190.36 as permitted sender)
15               Received: smtp.mail=remetente@hotmail.com
16                         from BAY171-W83 ([65.54.190.61]) by bay0-omc1-s25.bay0.hotmail.com
17                         with Microsoft SMTPSVC(6.0.3790.4675); Wed, 22 Feb 2012 16:35:19
18                         -0800
19             Message-ID: <BAY171-W830CADCBEF9CC9977AE3A2DD650@phx.gbl>
20            Return-Path: remetente@hotmail.com
21           Content-Type: multipart/alternative;
22                         boundary="_fc338da9-6460-480f-ae0c-f59545fff555_"
23       X-Originating-IP: [111.112.113.114]
24                   From: Remetente <remetente@hotmail.com>
25                     To: <destinatario@gmail.com>
26                Subject: RE: RE: Re: RE: Boa Noite
27                   Date: Wed, 22 Feb 2012 21:35:20 -0300
28             Importance: Normal
29            In-Reply-To: <CueVCXLKMO9shg8DSa32O4mMDxg@mail.gmail.com>
30             References: <BAY171-W90A2682A6FA6EF1C1909F8DD650@phx.gbl>
31                         <CNZ5xUaNvbCD_oGZpMX7074e-Cg@mail.gmail.com>
32                         <BAY171-W950418859D7F6B71F651B4DD650@phx.gbl>
33                         <CueVCXLKMO9shg8DSa32O4mMDxg@mail.gmail.com>
34           MIME-Version: 1.0
35  X-OriginalArrivalTime: 23 Feb 2012 00:35:19.0792 (UTC) FILETIME=[055ED700:01CCF1C3]
```

Figura 5 – Cabeçalho de uma mensagem resultante de um diálogo

X Headers são campos de cabeçalhos iniciados pela letra X maiúscula seguido de um hífen, de caráter informativo, que podem ser extremamente úteis na identificação da autoria de um e-mail. Os *X Headers* mais comuns são:

"**X-Mailer:**" Indica qual o cliente de correio foi utilizado para compor a mensagem.

"**X-Yahoo-Post-IP:**", "**X-AOL-IP:**", "**X-Apparently-From:**", "**X-SenderIP:**", "**X-Originating-IP:**", etc. Indicam o endereço *IP* da conexão à *internet* que o usuário utilizou para o envio da mensagem. Se este usuário utilizou-se de um artifício qualquer para encobrir seu endereço *IP* real, o conteúdo não terá nenhum valor.

"**X-OriginalArrivalTime:**" Informa a data e hora do envio da mensagem no fuso (*UTC*) seguido dessa mesma informação no formato *Windows Filetime*, que consiste em um valor de 64 *bits*

representado pelo número de intervalos de 100 nano segundos a partir de 01 de janeiro de 1601. Esse valor pode ser convertido para confirmação da hora real do envio e, associado ao endereço IP, indicarão o "**quando**" e "**onde**".

"Message-ID:" Este campo contém um identificador único gerado pelo primeiro servidor de correio que submete a mensagem (*MSA*) e tem um formato parecido com "***ID***"@"***HOST***", onde o ***ID*** constitui um identificador composto por uma sequência de caracteres (gerados por diversos algoritmos), inteligíveis ou não. ***HOST*** é o nome da máquina que gera o identificador. Se o *host* que gerou o **ID** fizer parte de um domínio, ***HOST*** será o nome do domínio. Se o ***Message-ID*** apresentar discrepâncias com o padrão A@B, como uma ***string* vazia**, **ausência do** "**@**" ou ainda apresentar um **nome de *host* diferente** do *MSA*, pode implicar na utilização de um servidor de correio eletrônico com *open relay,* diferente do domínio original do remetente ou uma mensagem forjada, como vimos na figura 3 do terceiro *post*.

Os campos *"In-Reply-To:"* e *"References:"* só aparecem quando uma mensagem é respondida ou encaminhada. O campo *"References:"* também pode ser utilizado para identificar uma conversação.

"**In-Reply-To:**" Contém o *Message-ID* da mensagem que está sendo respondida/encaminhada.

"**References:**" Contém o(s) *Message-ID*(s) da(s) mensagem(ns) que está(ão) relacionadas com a mensagem em análise.

Os campos *"Received:"* relacionam os servidores *MTAs* por onde passaram a mensagem, incluindo o *MSA* e o *MDA* (Ambos são *MTAs*). Este campo pode conter informações forjadas e se isso ocorrer, estas informações estarão sempre nos primeiros campos, já que há um empilhamento a partir do primeiro (base) até o último (topo) servidor.

O campo "**Received:**" possui a seguinte sintaxe:

Received: from "**A**" (Nome de **A** [IP de **A**])(Obs.) by **B** (Informações de **B**) via **C** with **D** id **E** for **F**; date-time

Onde **A** é o *host* de origem, **B** é o servidor que recebeu a mensagem e gera o campo "*Received:*", **C** é o protocolo, **D** é o serviço, **E** é o id gerado pelo servidor **B** e **F** é a conta do destinatário. *Date-time* é o instante em que ocorre a entrega da mensagem à B. As variáveis A, B, C, D, E e F podem não estar todas no conteúdo do campo, variando de acordo com cada situação. Vejamos alguns exemplos.

Exemplo 1:

```
Received: from estacao_remetente (unknown [110.111.112.113])
          (Authenticated sender: remetente@dominio_remetente.org)
          by dominio_remetente.org (Postfix) with ESMTPA id 3836010BF68EF
          for <  destinatario@dominio_destinatario.org >; Fri, 5 Jan 2012
          12:25:05 -0300
    FROM: remetente@dominio_remetente.org
      TO: destinatario@dominio_destinatario.org
    DATE: Fri, 5 Jan 2012 12:25:01 -0300
Message-ID: <442067891928B4FB4ADA3D69390304921@dominio_destinatario.org>
  X-Mailer: Microsoft Outlook Express 6.00.2900.5931
```

Figura 6: Campo "Received:" sem a variável "C"

Podemos dizer que neste caso a mensagem foi composta em um cliente de correio (*Microsoft Outlook Express 6.00.2900.5931*) instalado na "**estação_remetente**". Podemos ver que a estação não faz parte de um domínio pois o *Message-ID* tem como "***HOST***" a "**estação_remetente**". Caso a estação fizesse parte de um domínio (por exemplo: **dominio_destinatario.org**), o "***Message-ID:***" *teria como valor <44206789192B4FB4ADA3D69390304921@dominio_destinatario.org>*.

Exemplo 2:

```
Received: by 10.112.27.68 with SMTP id r4csp7586lbg;
                  Sun, 11 Mar 2012 16:12:42 -0700 (PDT)
```

Figura 7: Campo "Received:"

Este campo "**Received:**" da figura 7 não apresenta o *host* de origem (A) porque o *host* de destino (B) está no mesmo domínio de A.

Exemplo 3:

```
Received-SPF: pass (u1.dominio_remetente.org: domain of dominio_remetente.org
              designates 120.121.122.123 as permitted sender) client-
              ip=120.121.122.123; envelope-from=remetente@dominio_remetente.org;
              helo=estacao_remetente;
    Received: from estacao_remetente (unknown [111.112.113.114]) (authenticated
              user remetente) by u1.dominio_remetente.org (Postfix) with ESMTP id
              3836010BF68EF; Fri, 5 Jan 2012 12:25:05 -0300
        FROM: remetente@dominio_remetente.org
          TO: destinatario@dominio_destinatario.org
        DATE: Fri, 5 Jan 2012 12:25:01 -0300
  Message-ID: <44206789192B4FB4ADA3D69390304921@dominio_destinatario.org>
    X-Mailer: Microsoft Outlook Express 6.00.2900.5931
```

Figura 8

O campo "**Received-SPF:**" indica que o servidor implementou o *SPF* (*Sender Policy Framework*). O *SPF* é um padrão aberto que especifica um método técnico para evitar a falsificação endereço do remetente (envelope), comumente chamado de *return-path*, que é utilizado pelos *MTAs* para enviar a mensagem de um para o outro especificando o endereço de retorno em caso de falha. O *SPF* dificulta a utilização de endereços forjados através de políticas de permissão de envio de mensagens oriundas de domínios confiáveis.

Veja que o campo "**Received:**" identifica o nome do *host* remetente através do comando *HELO* ou *EHLO* e o registra como "**estação_remetente**" e identifica o usuário que utilizou sua conta ("**remetente**") para autenticar no domínio e enviar a mensagem. O *host* tem sua identidade registrada no campo "**Received-SPF:**" quando aponta o resultado do comando *HELO*.

No próximo *post* faremos uma análise em um cabeçalho de uma mensagem eletrônica.

Para saber nais sobre campo "**Received-SPF:**" visite o *site* do *Sender Policy Framework*

Considerações finais

Para finalizar a nossa série de *posts* sobre rastreamento de *e-mails* vamos analisar um caso real no qual, para preservar identidades, as pessoas e domínios envolvidos tiveram seus nomes trocados.

Um empresário recebe uma mensagem de correio eletrônico de um indivíduo que dizia conhecer uma pessoa que possuía segredos comerciais da empresa. Disse ainda que tinha acesso ao material e que poderia intervir caso o empresário lhe desse uma “pequena contribuição” em dinheiro. Para dar credibilidade à mensagem o indivíduo anexa cópia de um projeto sigiloso da empresa ao qual ele teve acesso. Vejamos o cabeçalho da mensagem recebida:

```
1               Return-Path: <extorsao@bol.com.br>
2                  Received: from a2-salsa3.bol.com.br ([200.147.35.114])by
3                            dominio.empresario.com.br(dominio.empresario.com.br)
4                            (MDaemon PRO v10.0.5)with ESMTP id md50004592163.msg for
5                            <empresario@dominio.empresario.com.br>; Thu, 10 Mar 2011 12:30:30 -
6                            0300
7                            dominio.empresario.com.br
8    Authentication-Results: spf=pass smtp.mail=extorsao@bol.com.br; x-vbr=hardfail header.vbr-
9                            info=bol.com.br (domain not recognized)
10              Received-SPF: pass (dominio.empresario.com.br: domain of extorsao@bol.com.br
11                           designates 200.147.35.114 as permitted sender) x-spf-
12                           client=MDaemon.PRO.v10.0.5
13                           receiver=dominio.empresario.com.br client-ip=200.147.35.114
14                           envelope-from=<extorsao@bol.com.br> helo=a2-salsa3.bol.com.br
15                 Received: from localhost (localhost.localdomain [127.0.0.1]) by a2-
16                           salsa3.bol.com.br (Postfix) with ESMTP id C854C2E807C;
17                           Thu, 10 Mar 2011 12:27:49 -0300 (BRT)
18                 Received: from a2-salsa3.adm.intranet (localhost.localdomain [127.0.0.1])
19                           by a2-salsa3.bol.com.br (Postfix) with ESMTP id AA6C62E804D;
20                           Thu, 10 Mar 2011 12:27:46 -0300 (BRT)
21            DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=bol.com.br; s=afl;
22                           t=1299770868; bh=mD21AR+0YWWEhIqN+mPftf6OnrKK01XOYgkdHMJ4zpA=;
23                           h=Date:From:To:Message-Id:In-Reply-To:References:Subject:
24                           Mime-Version:Content-Type;
25                           b=IEp7KOktpEqyIAPKZnOZ3lGgU647eqFoWEBwsmFYgjzcZJVZ9l3s9A8MX/DB4aaC3
26                           ONKgN7lythBRspdrudEoaf++eoEtkrd3UVNKD4nn3DxSGLBYXKTPEoE5r5upG79/Ar
27                           Bhuk7dgRExSfgAhjAcuzGzNoT4nBXArRPBZqdixQ=
28                 Received: from localhost.localdomain (a2-wextor9.host.intranet
29                           [10.129.136.226]) by a2-salsa3.adm.intranet (Postfix) with ESMTP id
30                           44C4CC8806E; Thu, 10 Mar 2011 12:27:46 -0300 (BRT)
31                     Date: Date: Thu, 10 Mar 2011 12:27:46 -0300
32                     From: "extorsao" <extorsao@bol.com.br>
33                       To: empresario@dominio.empresario.com.br
34               Message-ID: <4d78edf240c3e_4b4c856c83825c@a2-winter9.tmail>
35               References: <WC20110309180943.928584@dominio.empresario.com.br>
36                           <BAY146-w347CFE3974AE2BBEC4DBDEB4C80@phx.gbl>
37                           <BAY146-w50D443591448D66181621AB4C80@phx.gbl>
38                  Subject: proposta
39             MIME-Version: Mime-Version: 1.0
40             Content-Type: multipart/mixed; boundary="mimepart_4d78edf240cb3_4b4c856c8383ba"
41                 Reply-To: extorsao@bol.com.br
```

Figura 9: Cabeçalho completo da mensagem

Vamos nos deter inicialmente nos campos de cabeçalho situados entre as **linhas 28 e 34**.

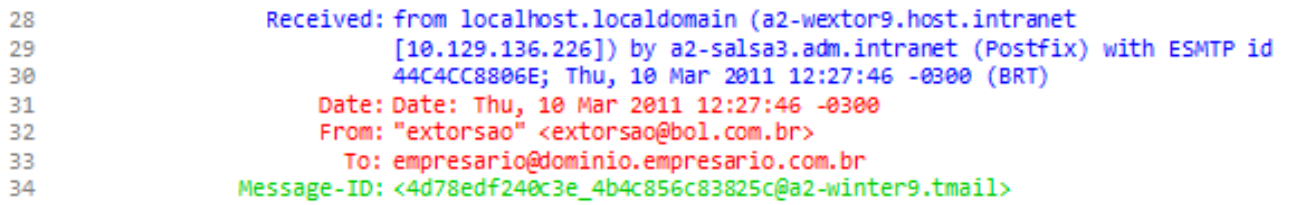


Figura 10: Linhas 28 a 34 do cabeçalho

Como podemos ver nas **linhas 31, 32 e 33** do cabeçalho, no dia 10/03/11, às 12:27:46 (hora local), o empresário recebeu em seu endereço de correio eletrônico **empresario@dominio.empresario.com.br** a tentativa de extorsão originada do endereço **extorsao@bol.com.br**, cujo valor do identificador **"Message-ID:"** presente na **linha 34** é **4d78edf240c3e_4b4c856c83825c@a2-winter9.tmail.**

O domínio **a2-winter9.tmail** associado ao campo **"Received:"** visto nas **linhas 28, 29 e 30**, nos indica que a mensagem foi composta através do *webmail* do BOL, pertencente ao UOL. O domínio **a2-winter9.tmail** é do BOL e o campo **"Received:"** nos indica que o primeiro MTA é **a2-salsa3.adm.intranet** uma máquina interna do BOL e que recebeu a mensagem do MUA **localhost.localdomain (a2-wextor9.host.intranet [10.129.136.226])** da mesma *intranet*. Logo a mensagem parece ser autêntica.

Vamos ampliar um pouco a área de análise. Vejamos o trecho contido entre as **linhas 28 e 38**.

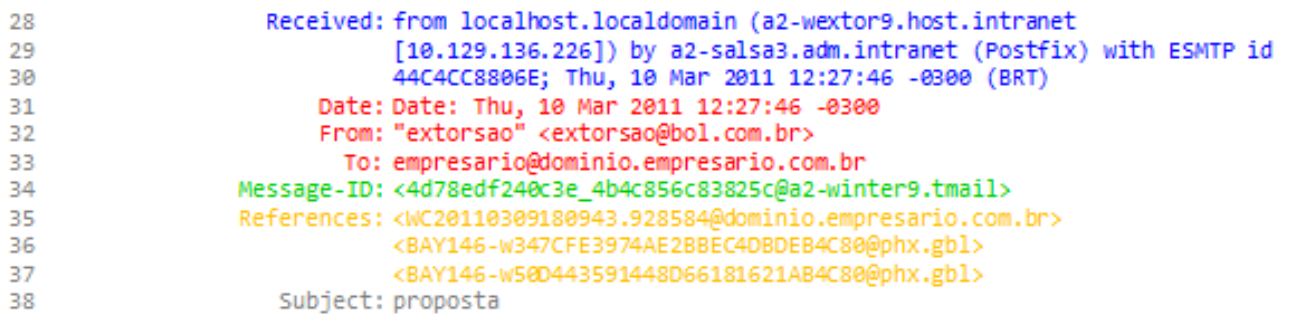


Figura 11: Linhas 28 a 38 do cabeçalho

No trecho compreendido entre as **linhas 35 e 37** podemos ver, através dos valores do campo **"References:"**, que a mensagem teve três encaminhamentos antes de chegar à caixa de mensagem do indivíduo desconhecido. O campo **"References:"** guarda o fio do diálogo, seja ele encaminhamentos ou respostas. Conforme podemos ver à **linha 34**, cujo valor é **WC20110309180943.928584@dominio.empresario.com.br**, o primeiro identificador foi gerado no domínio da própria empresa da vítima através do cliente de *webmail* Word Client, do MDaemon. A seguir vamos decompor o identificador e analisar as informações nele contidas.

Figura 12: Decomposição do campo “Message ID:” do MDaemon

Sabendo que o domínio era o da empresa da vítima solicitamos a ela o *log* de *SMTP* do *MDaemon* na data de criação da mensagem. A análise deste *log* nos mostrou que:

```
1  START Event Log / MDaemon PRO v10.0.5, SMTP (out) log information
2  --------------------------------------------------------------------------------
3  Event Time/Date             Event Description
4  --------------------------------------------------------------------------------
5  ...
6  Wed 2011-03-09 15:09:50: ----------
7  Wed 2011-03-09 15:09:50: Session 2769; child 1
8  Wed 2011-03-09 15:09:48: Parsing message <c:\mdaemon\queues\remote\pd35001130507.msg>
9  Wed 2011-03-09 15:09:48: *  From: funcionario@dominio.empresario.com.br
10 Wed 2011-03-09 15:09:48: *  To: fakemail@hotmail.com
11 Wed 2011-03-09 15:09:48: *  Subject: desvio de info
12 Wed 2011-03-09 15:09:48: *  Size (bytes): 15535
13 Wed 2011-03-09 15:09:48: *  Message-ID: <WC20110309180943.928584@dominio.empresario.com.br>
14 Wed 2011-03-09 15:09:48: Attempting SMTP connection to [hotmail.com]
15 ...
16 Wed 2011-03-09 15:10:50: ----------
17 Wed 2011-03-09 15:11:14: Session 2789; child 2
18 Wed 2011-03-09 15:11:10: Parsing message <c:\mdaemon\queues\remote\pd35001130506.msg>
19 Wed 2011-03-09 15:11:10: *  From: funcionario@dominio.empresario.com.br
20 Wed 2011-03-09 15:11:10: *  To: funcionario@bol.com.br
21 Wed 2011-03-09 15:11:10: *  Subject: desvio de info
22 Wed 2011-03-09 15:11:10: *  Size (bytes): 15531
23 Wed 2011-03-09 15:11:10: *  Message-ID: <WC20110309180943.928584@dominio.empresario.com.br>
24 Wed 2011-03-09 15:11:10: Attempting SMTP connection to [bol.com.br]
```

Figura 13: trechos de interesse do log do “MDaemon”

Chamado, o funcionário não só confessou como também apontou a participação de um colega de trabalho que havia tido a idéia e, a partir dos anexos recebidos do primeiro, compôs o texto da mensagem enviando-o de volta para que fosse enviado ao empresário, explicando assim a existência dos três identificadores.

O trabalho com mensagens de correio eletrônico requer além do conhecimento técnico, criatividade para elaborar cenários e com isso poder avaliar as possibilidades que cada caso lhe apresentará.

Para saber mais leia as RFCs relacionadas ao tema, principalmente as de número 2184, 2231, 2646, 2049, 2076, 2821, 2822, 3023, 3798, 4408, 5147, 5335, 5536, 6532 e tantas outras.