CRIMES CIBERNÉTICOS: NOÇÕES BÁSICAS DE INVESTIGAÇÃO E AMEAÇAS NA INTERNET

Waldek Fachinelli Cavalcante

1. Introdução

O presente trabalho tem por fim fornecer informações básicas sobre a investigação de crimes cibernéticos e despertar aqueles que militam no combate ao crime para a necessidade de investimentos intelectuais e estruturais nesta área, consciente que a complexidade do tema não permite aprofundamentos neste espaço.

Para este estudo, utilizar-se-á a definição de crimes cibernéticos como aqueles praticados com o auxílio da internet, os quais têm tido um crescimento exponencial, seja pelo aumento do número de usuários da rede, pelas falhas de segurança desta ou por inabilidade ou negligência no seu uso.

Outros conceitos mais amplos existem, como o que define os crimes cibernéticos como aqueles em que, para a conduta, utiliza-se de um computador, de uma rede ou de um dispositivo de hardware.[1]

É de se ressaltar que há crimes que podem ser praticados tanto por intermédio do acesso à rede mundial de computadores, como por outros meios; assim com há crimes que somente podem ser praticados no meio cibernético.

A infinidade de possibilidades de emprego da internet tem feito com que mesmo crimes considerados clássicos, se assim se pode dizer, possam também ser cometidos no ambiente virtual.

Basta imaginar a invasão remota dos computadores de um hospital, mudando as prescrições de receitas de remédios, ou o desligamento de

[1] Norton by Symantec. O que é crime cibernético? Disponível em: <http://br.norton.com/cybercrime-definition/promo> Acesso em 1 de junho. 2013.

aparelhos ou da fonte de energia elétrica, o que pode ser feito para cometer homicídios.

O mesmo ocorre com os furtos a bancos, que tanto pode ser cometidos por meio da web como pela entrada física na agência bancária.

Já o crime de invasão de dispositivo informático, previsto na recente lei brasileira 12.737/12, é um crime exclusivamente cibernético, haja vista que será praticado somente com a utilização de computadores e outros dispositivos de acesso à internet.

O tema é intrincado. A utilização da rede tem se popularizado com diferentes, úteis e maravilhosas funções, contudo, a falta de regulamentação e seu caráter transnacional se tornaram um desafio para a segurança e a investigação de crimes praticados na rede mundial de computadores e até mesmo para a soberania dos países.

2. A internet

Desenvolvida a partir da década de 60 do século passado, inicialmente para emprego militar, sua ideia central é uma reunião mundial de computadores interconectados, os quais se comunicam através do protocolo TCP\IP organizador das mensagens de dados entre os computadores.

Este protocolo é um conjunto de regras que permite dividir uma mensagem em pacotes trafegáveis pela internet que podem seguir diferentes caminhos pela rede, assim, se parte da rede estiver inoperante, os dados procurarão outro caminho e, como consequência, a grande rede continua a funcionar, mesmo se um de seus braços não estiver funcionando.

Aqui o brilhantismo da web, pois os dados podem procurar diferentes caminhos para chegar ao destinatário, sendo a mensagem partilhada em diversos pacotes que podem seguir estas diferentes vias de tráfego, até chegar ao destino, que tem um endereço numérico, chamado endereço IP. O TCP permite a reconstrução da mensagem no seu local de destino.

Logo, vários computadores podem trocar informações por várias conexões diferentes. E a rede foi se ampliando com o tempo, conectando mais e mais computadores, tornando-se a grande teia que temos hoje, sem um órgão central que a controla, pois é a união de diferentes redes independentes.

Importante frisar que esta grande rede não tem um único controlador, na verdade, é uma realidade sem fronteiras, desafiante para um mundo que historicamente se divide.

A conexão entre os computadores pode se dar por diferentes tecnologias, sendo que, com o advento da banda larga as principais formas de conexão são a ADSL, cabo, rádio, 3G, 4G, satélite e por fibra ótica.

Para enviar requisições para a internet, há que estar instalado no computador pessoal um programa de navegação (browser), sendo o acesso feito por meio de um modem, ligado a uma linha telefônica ou a um cabo (ou outras tecnologias), passando pela central telefônica, provedor e podendo ganhar o mundo por meio de cabos submarinos ou satélites.

Os dados que buscamos na *web*, em regra, estão disponíveis em *sites*, estes estão locados em computadores constantemente ligados à internet, denominados servidores. *Sites* e páginas são reconhecidos por um endereço número, o endereço IP.

Aquele conjunto de caracteres que digitamos no programa de navegação tem o nome de URL (*Uniform Resource Locator* – Localizador Uniforme de Recursos). Estes nomes de *sites* têm uma estrutura chamada nomes de domínio, que são atribuídos às páginas para facilitar sua identificação, caso contrário teriamos que guardar aquela sequência de números atribuídos às páginas, o número IP delas.

O www do endereço URL tem o papel de direcionar o endereço URL para a *world wide web* e não faz parte do nome de domínio. Após o www vem o nome do *site*, depois um sufixo do tipo de entidade, após, a sigla do país. Há variantes, como o caso dos *sites* sediados nos EUA que não possuem a extensão final, contudo esta é a regra básica.

Além das páginas da internet possuírem um número IP (*Internet Protocol*), toda vez que se conecta à internet, o usuário também recebe um número IP, exclusivo do utilizador durante a sua navegação. Por meio deste número, o navegante pode ser localizado.

Por esta característica, o endereço IP se torna uma evidência de extrema importância na investigação de crimes cibernéticos.

3. Riscos na internet

Além dos crimes cibernéticos, em si, trazemos neste tópico advertências sobre outros riscos na rede.

Engenharia social: denomina-se engenharia social um conjunto de habilidades utilizadas com o intuito de se conseguir que uma vítima potencial forneça dados pessoais ou realize uma tarefa ou execute um programa.

Em geral, para conquistar seu objetivo, se abusa da ingenuidade do alvo ou se procura ganhar a sua confiança, utilizando-se, por exemplo, de símbolos de instituições confiáveis, como órgãos públicos, grandes empresas etc para obter informações desejáveis ou invadir computadores.

Geralmente, o criminoso influencia a vítima utilizando-se de sentimentos de medo, ambição, curiosidade, solidariedade, montando uma armadilha.

Vírus de *boot*: um dos primeiros a serem desenvolvidos, é um programa que provoca danos em computadores, ficando alojado na parte de inicialização do computador, causando transtornos aos usuários quando dão partida no seu aparelho.

Vírus *time bomb*: caracteriza-se por prejudicar o funcionamento dos computadores em uma determinada ocasião. São desta modalidade os vírus sexta-feira 13, 1º de abril entre outros.

Vírus *worm*: tem como principal característica se multiplicar automaticamente, consumindo recursos do equipamento onde está instalado,

afetando o funcionamento de redes e ocupando espaço no disco dos computadores.

Botnets: são computadores em que se hospedam programas maliciosos e que podem ser acessados remotamente por criminosos para realizar diferentes atividades no computador da vítima.

A vítima não sabe que o seu computador está infectado, contudo, está sendo utilizado remotamente por terceiras pessoas.

Muito comum a utilização desta técnica para ataques cibernéticos, como os realizados pelo grupo de nome *Anony*mous, que utilizam milhares de *botnets* para atacar seus alvos.

Deface: este é um tipo de ataque a *sites* que tem por fim desconfigurar a página de internet. É uma atuação semelhante a pichadores, que maculam e desconfiguram o design da página alvo.

Vírus cavalo de troia: com atuação semelhante à mitológica, este arquivo malicioso se insere na máquina atacada permitindo que se acesse remotamente o computador alvo e se obtenha as informações que se deseja, as quais são remetidas para o criminoso.

Com a instalação do cavalo de troia, o invasor pode obter senhas, destruir ou captar informações, ter acesso ao que é digitado, controlar totalmente o computador etc.

Keylogger: é um software que tem a capacidade de registrar o que é digitado pelo usuário do computador invadido. Geralmente utilizado para coletar informações da vítima com o objetivo de o criminoso ter matéria prima para suas ações ilícitas.

Hijacker: é um programa que tem por fim controlar o navegador de internet, abrindo páginas sem o pedido do usuário ou páginas diferentes daquela digitada. Ainda podem abrir automaticamente pop-ups que geralmente são armadilhas para o usuário da internet, direcionando a vítima para sites falsos ou que tenham fins ilícitos.

Sniffers: são programas que têm por fim monitorar os dados transmitidos em uma rede. É uma forma de interceptação telemática, com ela, as informações que trafegam pela rede podem ser capturadas e analisadas para diversos fins criminosos, obtendo-se informações sensíveis. É uma forma eficaz de espionagem.

Backdoor ou porta dos fundos: é um programa que permite ataques e invasões ao computador.

Phishing Scam: é a técnica que tem por fim obter dados a respeito do usuário de um computador. Nasceu este tipo de fraude com a remessa de e-mail para a vítima que fomentava o acesso a *sites* fraudulentos, com o fim de captar informações bancárias, senhas e outros conteúdos relevantes.

As ações mais comuns de *phising scam* são as mensagens com links para vírus, páginas comerciais ou de bancos falsas e envio de formulários para o fornecimento de dados do usuário.

Todas estas ameaças indicam que a melhor alternativa para o seu combate é a prevenção, tomando atitudes para evitar a contaminação de computadores, treinamento dos usuários de redes, mantendo os programas atualizados, evitando abrir mensagens ou entrar em *sites* suspeitos, controle sobre quem acessa as máquinas e principalmente atenção, fugindo da negligência.

4. A apuração de *cybercrimes*

Há inúmeras formas de se praticar um crime cibernético, haja vista o dinamismo da tecnologia da informação. Assim, fator essencial para o sucesso do trabalho do investigador é, ao tomar conhecimento da prática de um crime desta natureza, delinear qual foi a ferramenta que os criminosos utilizaram para a ação ilícita.

O crime pode ter se dado com a utilização de programas maliciosos, *e-mail, websites*, programas de transferência de informações, grupos de debate,

redes sociais, *sites* de comércio eletrônico, entre inúmeros outros. Conforme este meio, diferentes serão as técnicas para a descoberta da autoria.

Algumas particularidades marcam os indícios da prática desta natureza de crimes: são instáveis, ou seja, podem ser de maneira descomplicada apagados, alterados, perdidos; o acesso a tais vestígios é complexo, não são colhidos facilmente como em outros crimes; como a própria internet, têm natureza supranacional, haja vista que com uma rede mundial se pode praticar estes tipos de crimes de qualquer lugar do globo que tenha acesso à rede; as evidências são intricadas, não são de fácil leitura, pois são informações complexas para seu estudo, devido ao seu formato; não bastasse, entre as informações de relevo para a investigação, em geral há enorme quantidade de fluxo de dados legítimos, que devem ser separados, demandando maior esforço na análise criminal.

Diante desta complexidade, devido à limitação deste espaço e a necessidade de conhecimentos cada vez mais complexos frente à infinidade de recursos cibernéticos que vem sendo desenvolvidos, trataremos dos principais meios utilizados para a prática de *cybercrimes* e o caminho para a coleta das evidências de tais ações ilegais.

4.1 Os *logs*

Ao acessar a rede mundial de computadores ou usar seu computar, o operador em geral não tem ideia dos registros que são gerados com suas ações. Os caminhos que as informações percorrem, como os pacotes são gerados, como são remetidas e recebidas mensagens, endereços IP etc não são visíveis.

Os usuários não têm que lidar com esta complexidade, seu acesso é facilitado pelo interface dos dispositivos que opera, ficando a parte complexa por conta de programas que gerem a informação.

Contudo, praticamente toda ação na web é de alguma forma registrada. Seja o conteúdo dos dados acessados, remetidos, manipulados, seja onde,

quando, como se acessou estes conteúdos, gerando neste último caso os logs ou registros das ações.

Estes registros ou *logs* são essenciais para a investigação de crimes que têm a rede como cena, seja por meio de *sites*, de *e-mails*, redes sociais, *chats* ou qualquer outra tecnologia que use a internet.

Fazendo-se uma analogia, da mesma forma que são mantidos por concessionárias de telefonia ou operadoras de cartão de crédito uma série de anotações contendo o histórico de seu uso, o mesmo ocorre em relação ao uso da internet. Podemos afirmar de modo simplista que cada clique do mouse ou *enter* na internet é anotado, contendo a hora, duração, conta do usuário, endereço IP atribuído à operação.

Assim, diferentemente do que se tem no imaginário popular, não existe anonimato na internet, cada página da internet acessada pelo usuário é registrada, podendo se saber o local de onde foi acessada, com inúmeros outros dados.

4.2 Endereço IP

Das evidências que podem ser coletadas na investigação de *cybercrimes*, sem dúvida o endereço IP é uma das de maior relevo. O IP, endereço IP ou número IP (*Internet Protocol*) é a identificação das conexões de computadores ou redes locais com a internet.

A partir da descoberta da identificação da conexão criminosa, é possível se chegar ao local de onde se desencadeou o ato delitivo, abrindo oportunidade de se identificar os autores de crimes a partir da máquina que teve acesso à internet ou da rede utilizada.

Formado por uma sequência numérica, separada por pontos, tem a forma X.X.X.X, sendo que o X corresponde a números variáveis entre 0 e 255. Por exemplo, o número 200.221.2.45 é o número IP do *site* www.uol.com.br.

Seja na remessa de um correio eletrônico, seja a um *site* de internet, é atribuído um número de IP, o importante é saber que sempre que se fizer conexão à internet, será atribuído um número IP ao usuário.

Em geral, as grandes corporações como órgãos públicos, empresas e universidades possuem uma faixa de IPs estáticos, que não muda, já aos usuários domésticos, comumente as operadoras lhes atribuem um número de IP dinâmico, ou seja, a cada conexão receberá um número de IP.

Logo, para identificar quem utilizou um número de IP dinâmico é necessário solicitar às concessionárias do serviço quem utilizava o IP em determinado dia, horário e fuso horário. Em consequência, nas solicitações de informações encaminhadas aos provedores de internet, para se obter a quebra do sigilo dos dados telemáticos, estes dados são imprescindíveis.

Para se saber quem é o responsável pelo provimento da internet utilizada pelo criminoso, insere-se o número IP em *sites* como registro.br ou whois.sc. Identificando-se o provedor, se está mais perto do autor do crime, devendo solicitar ao concessionário do serviço de internet os dados do usuário procurado e outras evidências possíveis.

4.3 Investigações envolvendo *websites*

Para melhor explicar o acima narrado, passa-se a abordar a investigação de crimes envolvendo *sites* de internet e no próximo tópico crimes envolvendo correio eletrônico.

Apesar de inúmeros outros ambientes cibernéticos onde o crime possa ocorrer, concentra-se nestes dois, os mais comuns.

Quando o usuário digita no seu *browser* ou programa de navegação o endereço de domínio, este endereço é traduzido para um número IP. Assim, ao se digitar o endereço de domínio www.portadosfundos.com.br no navegador, este domínio é convertido no número 186.202.153.80.

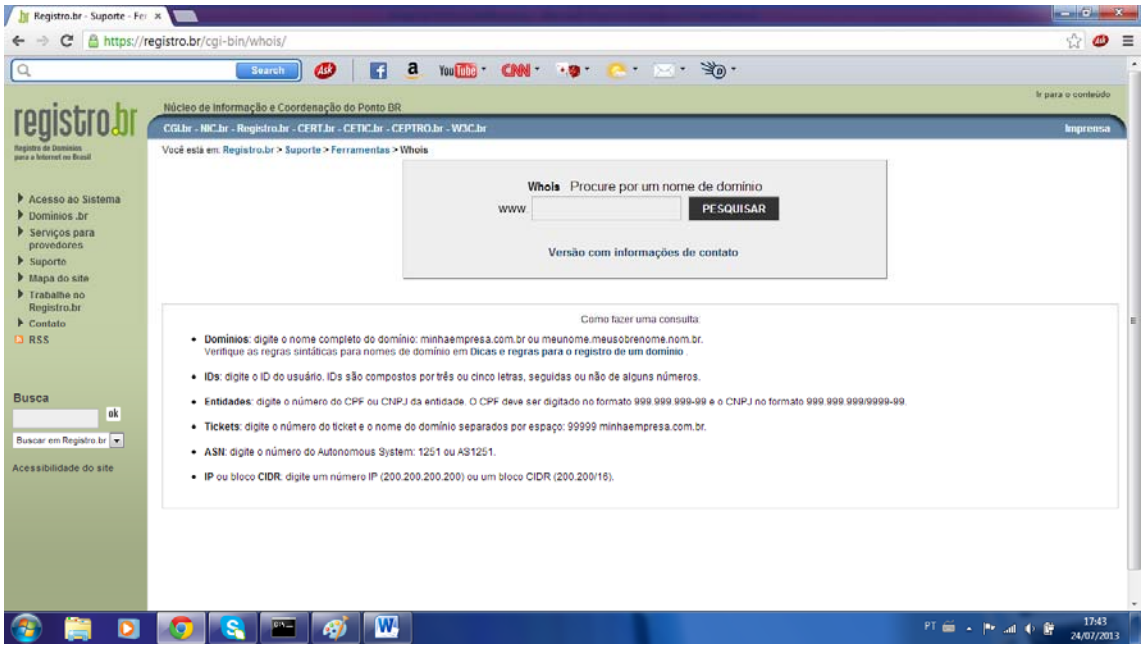
Ao se criar um *site*, o seu domínio (nome do *site*, nome de domínio, endereço do *site*) precisa ser registrado na internet. O Comite Gestor da Internet, por meio do Registro.br, é o responsável por este controle no Brasil, sendo que cada país tem um órgão encarregado para esta organização.

Para registrar o domínio, ele deve estar disponível, ou seja, não deve haver dois nomes de domínio iguais, em regra. Também há regras para a criação do nome de domínio, que são uma fonte de dados do seu proprietário. Um exemplo destas regras é cada país possuir sua terminação, como .br para o Brasil, ou .pt para Portugal, informações importantes para o investigador.

Para localizar na internet os gestores dos registros de nomes de domínio de cada país, pode-se acessar o *site* da IANA: www.iana.org/domains/root/db. Por meio desta ferramenta se pode buscar informações sobre os gestores de internet de cada nação.

Infelizmente, para a investigação, o registro de domínio na internet é muito descomplicado, facilitando fraudes, pois não há necessidade de se remeter ao gestor documentos dos responsáveis pelo *site* para se criar o nome de domínio.

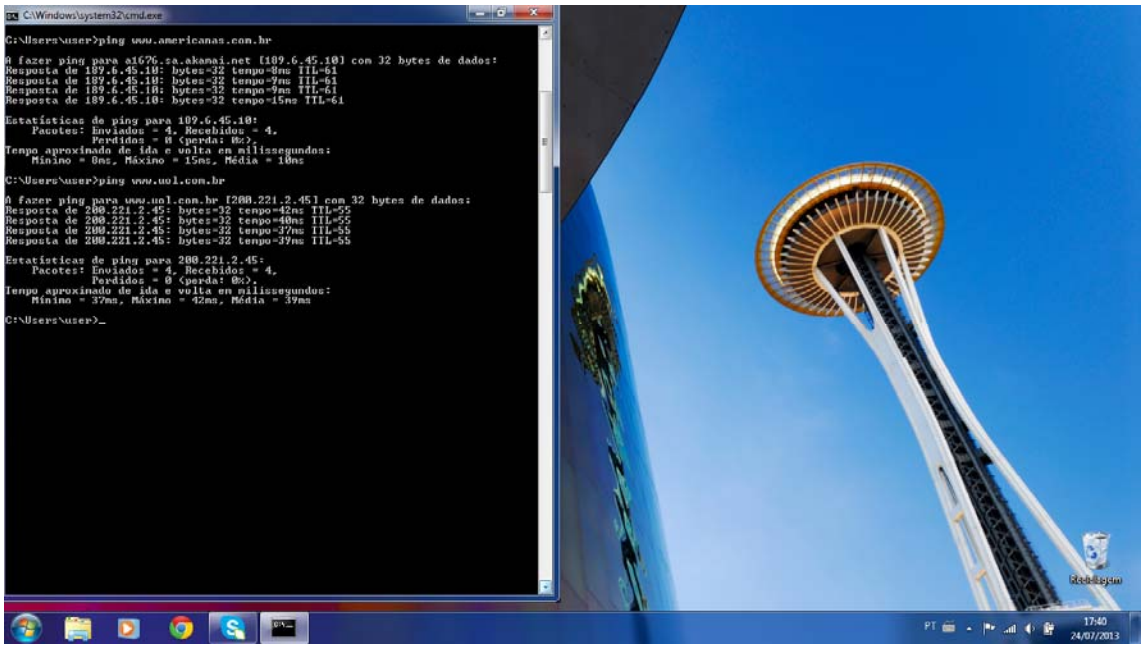
De uma forma ou de outra, para se obter informações sobre o responsável por um *site*, deve-se solicitar estas informações ao gestor de cada país, o que pode ser feito na própria internet, no *site* da IANA já comentado, ou no Brasil no site www.registro.br.



Para termos acesso ao cadastro do responsável por um *site* no Brasil, por exemplo, entramos em suporte/ferramentas/serviço de diretório *whois* do *site* www.registro.br onde podemos obter o cadastro por várias formas.

Podemos retirar inúmeros dados da pesquisa na ferramenta *whois*, tais como o responsável pelo domínio e seu registro tributário, o servidor responsável por manter o *site* ativo, contato técnico entre outros.

Importante lembrar que em geral os *sites* estão hospedados em computadores de empresas que prestam este serviço. Um meio para se obter informações sobre a hospedagem de um *site* é, nos computadores que utilizam o Windows, utilizar o comando PING. Vai-se em Iniciar – Executar – digita-se cmd – Enter. Ao se abrir uma tela preta, digita-se o comando PING – espaço – digita-se o nome de domínio – clica-se *enter*.



Com este comando teremos o endereço IP que identifica a hospedagem do *site* pesquisado.

De posse deste número IP, vai-se à ferramenta *whois* do Registro.br e se obtem os dados do provedor do serviço de hospedagem.

Com estas evidências, podemos chegar a autores de crime, solicitando aos provedores os logs e outros dados utilizados por criminosos. Estas mesmas informações podem ser utilizadas para coletar dados através de busca eletrônica em fontes abertas, tal como o *site* de busca do Google.

Importante o investigador estar atento a todo tipo de conteúdo exposto no *site* investigado, pois pode encontrar a presença de indício importante, como o *e-mail* dos responsáveis pelo *site*, números de telefone, ou mesmo conteúdo de conversas que podem facilitar o trabalho policial.

Outros *sites* que podem ser utilizados para pesquisas relativas a domínios são whois.domaintools.com, robtex.com/dns, 100br.com/whois.completo.php, cqcounter.com/whois, dndetails.com/index.php, ip-adress.com/whois entre outros, sendo que este último traz a geolocalização da hospedagem e rastreamento de origem de correio eletrônico.

Como as evidências de crimes envolvendo *sites* de internet são voláteis, não basta ter o endereço de domínio, há que se fazer a impressão do conteúdo

do *site*, das páginas que contém os indícios de crime, ou, mais útil ainda para a investigação, fazer o download do conteúdo de interesse, haja vista que as páginas podem ser apagadas ou alteradas, perdendo-se as provas necessárias para a localização e condenação de autores de crimes.

A manutenção da originalidade do conteúdo do *site* investigado tem além do objetivo de ter estes dados como fonte para a localização dos criminosos, também evitar possíveis questionamentos no processo penal sobre a integridade destas informações e se elas não foram alteradas no curso da investigação.

Logo, o ideal é fazer o download das páginas com o uso de ferramentas que produzem uma assinatura digital, com a qual se pode constatar a originalidade do conteúdo capturado. Isto pode ser feito com intrumentos como o HTTrack, Wget, WinMD5 .

4.4 Investigação de crimes envolvendo *e-mail* (correio eletrônico)

Quando o indício de crime estiver em mensagem de *e-mail*, como, por exemplo, injúrias, difamações, calúnias, pornografia infantil, programas maliciosos, deve-se preservar não só o conteúdo criminoso ou que foi utilizado para cometer crimes, mas também os dados do destinatário e remetente da correspondência, o chamado cabeçalho do e-mail.

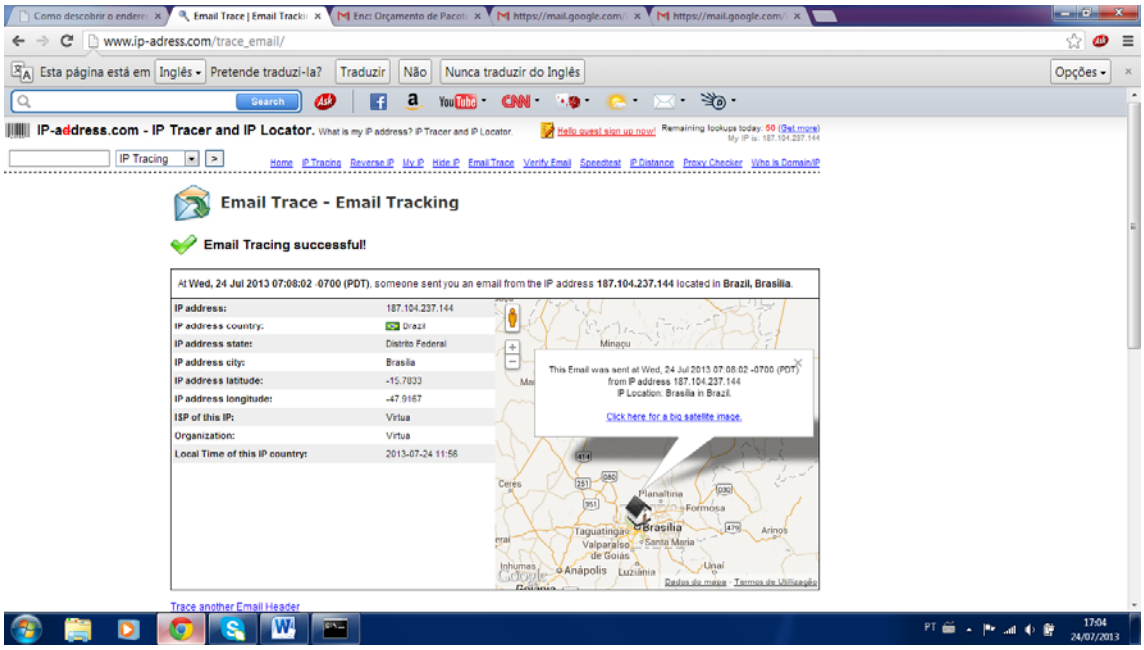
Este cabeçalho é de suma importância para a investigação, por intermédio de seu conteúdo se poderá chegar à origem da mensagem. Contudo, deverá se fazer a expansão do cabeçalho para se ter acesso ao seu pleno conteúdo, fundamental para identificar de onde partiu o correio eletrônico.

Ao se analisar o cabeçalho, as principais informações a serem colhidas são o endereço IP, a data, hora e *timezone* de envio da mensagem, o que não pode ser burlado, já que outros dados do remetente podem ser falsos.

A expansão do cabeçalho pode, em geral, ser feita com alguma ferramenta disponibilizada pelos provedores de contas de e-mail, porém, cada um possibilita esta expansão de forma diferente. Deve ser feita a análise caso a caso, para se obter a expansão.

Assim, se o *e-mail* for recebido em uma conta do provedor GMAIL de serviço de correio eletrônico, na parte superior direita há uma seta, clicando sobre ela aparecerão várias opções, clica-se então sobre mostrar original, ter-se-á então o cabeçalho expandido, o que até assusta pela forma não muito amistosa da informação.

Contudo, para facilitar a leitura das informações ali presentes, pode-se copiar este cabeçalho expandido e colar na ferramenta disponível na internet no *site* www.ip-adress.com/trace-email, esta ferramenta de leitura de cabeçalho também está disponível em outros *sites* abertos. Após colar, clica-se em *trace e-mail*, com este comando o *site* dará informações mais "limpas" quanto ao conteúdo do cabeçalho.



Um exemplo de resultado está na imagem acima, com inúmeras informações de forma bem didática sobre a origem da mensagem analisada, inclusive com localização geográfica.

Em *e-mail* do Hotmail, o cabeçalho expandido é obtido clicando no desenho de engrenagem, após, clicando em exibir cabeçalho completo. Então, copia-se e cola no trace *e-mail*, obtendo as informações buscadas.

Com estes dados, solicitam-se ao provedor os dados cadastrais do usuário a quem foi fornecido aquele número IP, na data e horário obtidos, devendo haver especial atenção quanto ao fuso horário.

Não sendo possível acessar o cabeçalho de um *e-mail*, mas tendo uma conta de *e-mail* a ser investigada, pode-se solicitar o provedor do serviço de correio eletrônico (ex: Microsoft, Google, Pop, Uol, Yahoo, Facebook) informações cadastrais e registros de eventos da conta de *e-mail* (estes registros são o *logs*, que conterão quais endereços IP tiveram acesso à conta, com data, hora e fuso).

Com a resposta do provedor de conta de *e-mail*, procura-se um *site* de leitura de IPs, como já citados, tais como www.en.trace.de ou www.registro.br e encontra-se qual o provedor de internet que forneceu aqueles IPs. De posse do nome deste provedor de internet, solicita-se a este os dados cadastrais de quem usou o IP por ele fornecido no dia, hora e fuso fornecidos pelo provedor de conta de *e-mail*, então, poder-se-á chegar à localização física de quem teve acesso a uma conta de *e-mail*, da qual não havia qualquer informação inicialmente.

4.5 Interceptação telemática

A interceptação telemática tem lugar quando se quer obter todo o trânsito de dados de internet do investigado. Para isto, há que se conhecer todas as formas de acesso do alvo à rede mundial de computadores, seja no seu local de trabalho, na sua residência, em instituição de ensino, no smartphone ou outro meio, para que se possa, por intermédio do provedor de internet de cada um destes ambientes, realizar-se a interceptação da comunicação de dados.

Diferentemente da interceptação de comunicações telefônicas, a interceptação telemática tem se mostrado muito mais complexa, seja pela falta de padronização dos provedores na forma de disponibilizar o tráfego de informações do investigado, seja pelo conteúdo final do fluxo. Na interceptação telefônica temos um produto mais simples, a conversação de voz, a qual é captada como a original. Já na telemática, os dados em trânsito devem ser remontados, não sendo captado cada movimento da tela do computador, o que só poderia ser feito com técnicas de intrusão.

No caso de contas de *e-mail*, os provedores deste serviço podem fornecer uma “conta espelho”, contendo todas as mensagens recebidas e enviadas pelo investigado, ficando a senha desta conta à disposição do investigador.

4.6 Redes sociais *online*

As redes sociais *online* são um fenômeno que tem crescido juntamente com a internet, devido a inúmeras utilidades agregadas a ela. Ao mesmo tempo, tem servido de refúgio de criminosos, fazendo uso destes recursos de inúmeras formas, sempre buscando o anonimato aparente da rede.

A principal rede social do globo possui mais de um bilhão de pessoas cadastradas, unidas por diversos tipos de relações, trocando dados, conhecimentos, informações no âmbito global, permitindo a agregação e desagregação de membros.

Mais e mais estas redes sociais ganham importância, servindo para todo tipo de fim, desde busca de relacionamentos amorosos, passando por interesses empresariais, até a espionagem, terrorismo, guerra e protestos, fazendo até certos serviços tenderem a ficar obsoletos, como o correio eletrônico tradicional e as ligações telefônicas.

Em consequência, o crime, desde o mais banal, até o crime organizado transnacional tem feito uso destas comunidades.

Infelizmente, os usuários destas redes muito se expõem, facilitando ataques ilícitos, assim como é uma constante a presença de crianças e adolescentes, os quais são vítimas potenciais de crimes, devido a maior abertura para contatos virtuais.

Diante da ocorrência de fato criminal no âmbito da rede social *online*, o responsável pela investigação deverá solicitar à pessoa jurídica responsável pelo *site* que forneça (em regra, com a necessidade de ordem judicial) os *logs* dos acessos criminosos, dados dos perfis dos usuários e grupos envolvidos, e, sendo necessária, a interceptação telemática do fluxo de dados.

Com isto, procede-se da mesma forma já descrita acima em relação à busca dos responsáveis pelos eventos ilícitos.

4.7 Busca eletrônica

Os avanços da internet não só propiciaram um novo desafio para as polícias e a sociedade diante dos crimes que envolvem seu uso, a rede mundial tem permitido também a aplicação de seus recursos para a solução de crimes os mais diversos, não só os *cybercrimes*.

Os *sites* de buscas, as redes sociais e inúmeros tipos de *websites* têm propiciado uma magnífica fonte aberta de informações úteis à investigação criminal.

Podemos até dizer que o mundo tornou-se mais transparente, diante da socialização da informação, principalmente por órgãos públicos e de imprensa, acessíveis a um toque na tela do computador.

Todo tipo de informação está mais acessível, inclusive dados de pessoas. As redes sociais, mormente diante da vaidade das pessoas que muito se expõem, tornaram-se uma fonte infindável de identificação de criminosos e localização de pessoas.

Além disso, abrem a oportunidade do uso destas fontes abertas para infiltração em grupos criminosos. Com perfis falsos, criados pelos investigadores, é possível se obter a confiança de membros de quadrilhas e obterem-se evidências necessárias para elucidar os mais diversos crimes.

5. Adversidades a serem superadas

Apesar dos desafios, soluções estão sendo procuradas, como as novas legislações, treinamentos para policiais, busca de cooperação policial e jurídica internacional, entre outras soluções necessárias para acompanhar o desenvolvimento de novos dispositivos que acessam a internet, a expansão desta, e o consequente surgimento de diferentes ameaças.

A criminalidade cibernética tornou-se um grande adversário da investigação, havendo necessidade de preparação das polícias, do ministério público e do judiciário para este enfrentamento.

Esta modalidade de crimes tem trazido imensos prejuízos para a sociedade, sendo que algumas dificuldades devem ser solucionadas para se adequar ao novo mundo.

5.1 Dificuldades para obter-se a origem de um evento na internet

A princípio, após a obtenção do endereço IP correspondente a uma ação na internet, ter-se-ia a identificação do local que originou o registro. Contudo, há meios de burlar esta evidência, como os *proxies*, as redes *wifi* abertas, os *cyber* cafés e *lan houses*, além do uso de documento falso em cadastros. Logo, o investigador deve estar atento a estes obstáculos.

Os *proxies* são serviços que ocultam o verdadeiro IP utilizado em um evento de internet, dificultando o rastreamento de quem realizou a conduta. Os servidores *proxy* acabam facilitando o anonimato na internet, apesar não terem somente fim ilícito.

Com o aumento da utilização de *smartphones, tablets* e computadores portáteis, mais redes sem fio ou redes *wireless* vão sendo instaladas, dando acesso gratuito à internet. Contudo, estas redes permitem o uso de pessoas não identificadas, o que é uma porta de oportunidades para criminosos, pois dificultam sua localização, assim como facilitam a intrusão para fins maliciosos.

Outra questão relacionada é a falta de registro de usuários que utilizam o serviço de internet nas denominadas *lan houses* e *cyber* cafés, assim como o uso de documento falso para preencher cadastros, seja para acesso a serviços de internet, seja para outros contratos relacionados com o crime investigado, como a abertura de contas bancárias.

Ainda quanto a dificuldade de rastreamento, fundamentais para a investigação e identificação do autor de um crime cibernético são os *logs* de acesso e conexão aos serviços prestados pelos provedores.

Como já dito, os logs são registros de toda a movimentação do usuário na internet, sendo então preciosa evidência. Contudo, não existe regulamentação da guarda destes eventos, o que prejudica ou inviabiliza o trabalho investigativo.

5.2 Legislação

Há necessidade de legislação mais sintonizada com a nova realidade. Alguns passos vão sendo dados no caso brasileiro, contudo, ainda tímidos diante da expansão da internet.

Estamos diante de uma problemática mundial, um embate entre a liberdade e a segurança na internet, contudo, poderíamos dizer que o mundo cibernético ainda é uma terra sem lei.

Só recentemente que foi aprovada, no Brasil, a Lei 12.737/12 que trata da tipificação criminal de crimes informáticos, a Lei 12.683/12 acrescentou o artigo 17-B à Lei de lavagem de dinheiro que para permitir a requisição de dados cadastrais sem necessidade de autorização judicial a provedores de internet.

Já a Lei 12.830/13, explicitou o poder de requisição de documentos pelo Delegado de Polícia, enquanto Projeto de Lei que aguarda sanção presidencial permite a obtenção destes dados cadastrais na investigação de organizações criminosas.

Contudo, é uma legislação ainda tímida, em verdade, a internet é muito pouco ordenada, exemplo é a falta de regulamentação da guarda de *logs*, o que facilita a atividade criminosa e prejudica ou inviabiliza a investigação.

5.3 Computação nas nuvens ou *Cloud Computing*

A computação nas nuvens é o serviço que permite o acesso a arquivos, programas e a execução de diferentes atividades pela internet. Com isto, estes dados não precisam estar no computador do usuário. Logo, se este quiser acessar um arquivo ou rodar um programa, não precisa tê-los no seu

computador, além de poder utilizá-los a partir de qualquer dispositivo ligado à internet.

Ou seja, funções, serviços, programas, arquivos ficam “na nuvem”, em computadores que têm a função de hospedar estas funcionalidades, não no computador do usuário da internet. Muitos destes servidores que mantém estes serviços para os usuários podem estar em outros países, a “nuvem”, estes computadores acessados remotamente, podem estar em um lugar muito diferente de onde esteja o usuário, inclusive além-fronteira.

Ou seja, em uma comparação leiga, é como se o HD do usuário não estivesse em seu computador, mas em um lugar que muitas vezes nem o usuário sabe, muitas vezes nem sabe que suas informações estão na nuvem. O *Dropbox* é um exemplo de computação nas nuvens, no que os arquivos levados ao *Dropbox* são duplicados no servidor hospedeiro.

Esta tecnologia, apesar da utilidade, sendo muito procurada por diferentes perfis de usuários, dificulta e muito a investigação, pois afinal, muita dificuldade haverá em apreender um computador que esteja em outro país (a “nuvem” em si), ou haverá demora destes provedores de serviço *cloud computing* em prestar informações, em retirar do ar *sites*, emperrando o serviço investigativo e tornando-se uma ameaça à segurança.

5.4 A preparação da Polícia, Judiciário e Ministério Público

Apesar da vasta aplicação e difusão, a internet e as tecnologias vinculadas a ela são muito recentes, o que faz que os órgãos investigativos e judiciários não estejam adequadamente preparados para lidar com esta nova criminalidade.

Em todos estes órgãos há agentes estatais sem qualquer conhecimento sobre as tecnologias, terminologias e necessidades envolvidas na investigação do *cybercrime*, vulnerando a sociedade.

Urge, então, a necessidade de preparo destes agentes para lidar ou, ao menos, ter noções básicas, de tecnologia, mormente os da área jurídica, para

ajudarem ou terem consciência dos desafios enfrentados por este tipo de investigação, prestando um melhor serviço à sociedade. Acresça-se a necessária estruturação das polícias para esta luta.

5.5 Cooperação internacional

A própria natureza transnacional da internet já indica a necessidade de cooperação internacional entre polícia e judiciário de diferentes países para enfrentar a criminalidade cibernética.

O fluxo de informações é internacional, a rede é internacional, os participantes da rede estão alocados nas diferentes partes do globo, as redes sociais são globalizadas, informações de cada país estão disponíveis a todo o mundo.

Em decorrência, as ameaças são globalizadas, o preparo, a execução e o resultado de um crime podem se dar em diferentes países. Criminosos cibernéticos de diferentes regiões do globo podem se unir para realizar ataques a partir de suas fronteiras.

E mais e mais isto ficará evidente com a expansão da internet, o aumento do número de usuários e o aumento de provedores de serviços para internet de alcance global.

Desse modo, para enfrentar uma modalidade de crime que não conhece fronteiras, todavia praticados em um mundo politicamente fragmentado, com legislações e estruturas distintas, a cooperação internacional entre os órgãos responsáveis pela persecução penal é indispensável, muitas vezes sob pena de impossibilitar o combate a infrações penais.

Contudo, esta cooperação ainda é extremamente burocrática, há a necessidade urgente de se aperfeiçoar a colaboração entre países para a repressão a crimes cometidos pela rede mundial de computadores, imprescindível um canal aberto entre as polícias e os órgãos judiciários para atender a velocidade de crimes que circulam por fibra ótica.

6. Conclusão

As informações aqui trazidas são básicas, havendo inúmeras variáveis a afetar a investigação de crimes cibernéticos, necessária ainda formação específica para lidar com determinadas tecnologias.

Porém, são noções que podem ser empregadas a uma infinidade de condutas criminosas virtuais.

A internet é símbolo da capacidade humana de progredir, uma revolução, um estouro de democracia e liberdade. É um instrumento de transformação do mundo que ainda não temos ideia do seu efeito para a comunidade global.

Uma ferramenta tão magnífica deve ser preservada de ameaças e seus usuários devem estar seguros. Este é o objetivo de se estudar como protegê-la.

Os desafios são grandes, os profissionais que labutam contra a criminalidade aqui apontada devem ser capacitados, devem ser elaboradas normas que protejam a rede de ameaças e torne menos tormentosa a coleta de dados para a identificação de criminosos.

A troca de informações entre órgãos dos diferentes entes federativos e entre estes e os provedores de serviços de internet deve ser célere, buscando-se maior profissionalismo e menor pessoalismo na investigação criminal.

Deve haver uma ampla regulamentação do setor, propiciando agilidade na prestação de informação por parte dos provedores de serviço de internet e a guarda de registros.

Por fim, como diz o ditado, a prevenção é o melhor remédio. O usuário, possível vítima de crimes, deve ser conscientizado e procurar se conscientizar dos riscos existentes no mundo conectado, protegendo-se.

Post scriptum: Gostaria de agradecer a Academia de Polícia Civil da PCDF e seus instrutores pelos cursos de investigação de crimes cibernéticos ministrados e material didático produzido; parabenizar os Delegados de Polícia Emerson

Wendt e Higor Jorge pela obra de referência que escreveram; e ao MPF pela cartilha confeccionada; bibliografia principal utilizada para este estudo.

BIBLIOGRAFIA

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal introdução à sociologia do direito penal**. 3. ed. Rio de Janeiro: Revan, 2002.

BRASIL. **Manual de cooperação jurídica internacional e recuperação de ativos**: cooperação em matéria penal. Brasília: Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, 2008.

CERT.br. **Cartilha de segurança para internet**. Disponível em:<http://cartilha.cert.br/>. Acesso em: 10.7.2013.

FEITOSA, Denilson. **Direito processual Penal**: Teoria, crítica e práxis. 7. ed. Niterói: Impetus, 2010.

HAMMERSCHIMDT, Roberto. **10 dicas para saber se um site é confiável.** Disponível em: < http://www.tecmundo.com.br/seguranca/1194-10-dicas-para-descobrir-se-um-site-e-confiavel.htm>. Acesso em: 10.7.2013.

JORDÃO, Fábio. **O que é IP estático? E dinâmico?** Disponível em: **<**http://www.tecmundo.com.br/1836-o-que-e-ip-estatico-e-dinamico-.htm>. Acesso em: 15.7.2013.

Ministério Público Federal. **Crimes cibernéticos:** Manual prático de investigação. São Paulo: Procuradoria da República no Estado de SP, 2006.

MULAS, Nieves Sanz. **El desafio de la criminalidad Organizada**. Granada: Comares, 2010.

Polícia Civil do Distrito Federal. **Curso básico de investigação de crimes cibernéticos**. Brasília: Academia de Polícia Civil do Distrito Federal, 2012.

UOLtecnologia. **Mitos e verdades sobre a segurança de seu computador**. Disponívelem:<http://tecnologia.uol.com.br/album/mitoseverdade_seguranca_album.htm#fotoNav=1>. Acesso em 25.7.2012.

VALENTE, Manuel Monteiro Guedes. **Teoria Geral do Direito Policial**. 3. ed. Coimbra: Almedina, 2012.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos**: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.